

Digital Safety Procedural Policy

(Name of Organization)

(Date of Last Update)

1. Purpose and Scope	5
2. Team Members	5
3. Digital Accounts Tracking	6
3.1. Purpose and Scope	6
3.2. Policy Statement	6
3.3. Digital Account Tracking Tool Selection	7
3.3.1. Approved Tools	7
3.3.2. Prohibited Tools	7
3.4. Account Management Practices	7
3.4.1. Account Creation	7
3.4.2. Account Monitoring	7
3.4.3. Account Reviews	8
3.5. Training and Support	8
3.5.1. Employee Training	8
3.5.2. IT Support	8
3.6. Data Security	8
3.6.1. Protecting Digital Assets	8
4. Digital Identity	9
4.1. Purpose	9
4.2. Scope	9
4.3. Policy Statement	9
4.4. Digital Identity Protection Practices	9
4.4.1. Account Security	9
4.4.2. Email and Communication Security	11
4.4.3. Social Media and Public Profiles	16
4.4.4. Doxxing and Public Information Protection	41
4.5. Personal Device Security	42
4.6. Incident Response and Reporting	44
4.6.1. Reporting Security Incidents	44
4.6.2. Organizational Response	44
4.7. Training and Awareness	44
	1

This document is published by the Open Digital Literacy and Access Network as an open source resource. For questions or modifications, please contact info@odlan.ca. This work is licensed under CC BY-NC 4.0.



4.7.1. Employee Training	44
4.7.2. Awareness Campaigns	45
5. Incident Response	45
5.1. Purpose	45
5.2. Scope	46
5.3. Crisis Response Team (CRT)	46
5.3.1. Team Composition	46
5.3.2. Contact Information	46
5.4. Incident Detection and Assessment	46
5.4.1. Detection	46
5.4.2. Assessment	46
5.5. Immediate Response Actions	47
5.5.1. Containment	47
5.5.2. Communication	47
5.6. Detailed Response	47
5.6.1. Public Communication	47
5.6.2. Technical Response	47
5.7. Recovery and Resolution	47
5.7.1. Restore Normal Operations	47
5.7.2. Post-Incident Actions	48
5.8. Post-Crisis Review	48
5.8.1. Incident Analysis	48
5.8.2. Policy and Procedure Updates	48
5.9. Ongoing Monitoring and Improvement	48
5.9.1. Monitor for Recurrence	48
5.9.2. Feedback and Improvement	48
6. Incident Response Strategy for Email Accounts Receiving Hate Mail	49
6.1. Purpose	49
6.2. Scope	49
6.3. Incident Detection	49
6.3.1. Indicators of Hate Mail	49
6.4. Immediate Response Steps	49
6.4.1. Employee Actions	49
6.4.2. IT Department/Security Team Actions	49
6.5. Containment and Mitigation	51
6.5.1. Contain the Threat	52
6.5.2. Mitigate Impact on Employees	52
6.6. Recovery and Communication	52
6.6.1. System Recovery	52
6.6.2. Internal Communication	52
6.6.3. External Communication	52



7. Email Phishing Incident Response Strategy	53
7.1. Purpose	53
7.2. Scope	53
7.3. Incident Detection	53
7.3.1. Indicators of Phishing	53
7.4. Immediate Response Steps	53
7.4.1. Employee Actions	53
7.4.2. IT Department Actions	53
7.5. Containment and Eradication	54
7.5.1. Contain the Threat	54
7.5.2. Eradicate the Threat	54
7.6. Recovery and Communication	54
7.6.1. System Recovery	54
7.6.2. Internal Communication	54
7.6.3. External Communication	54
8. Social Media Account Incident Response Strategy	55
8.1. Purpose	55
8.2. Scope	55
8.3. Incident Detection	55
8.3.1. Indicators of Compromise	55
8.4. Immediate Response Steps	55
8.4.1. Employee Actions (For those not responsible for platforms)	55
8.4.2. IT Department/Social Media Manager Actions	55
8.5. Containment and Eradication	56
8.5.1. Contain the Threat	56
8.5.2. Eradicate the Threat	56
8.6. Recovery and Communication	57
8.6.1. System Recovery	57
8.6.2. Internal Communication	57
8.6.3. External Communication	57
9. Incident Response Strategy for Social Media Account Dogpiling	57
9.1. Purpose	57
9.2. Scope	58
9.3. Incident Detection	58
9.3.1. Indicators of Dogpiling	58
9.4. Immediate Response Steps	58
9.4.1. Employee Actions	58
9.4.2. Social Media Team/Incident Response Team Actions	58
9.5. Containment and Mitigation	58
9.5.1. Contain the Threat	59
9.5.2. Mitigate Impact on Individuals	59



9.6. Recovery and Communication	59
9.6.1. Account Recovery	59
9.6.2. Internal Communication	59
9.6.3. External Communication	59
10. Website Attack Incident Response Strategy	60
10.1. Purpose	60
10.2. Scope	60
10.3. Incident Detection	60
10.3.1. Indicators of an Attack	60
10.4. Immediate Response Steps	60
10.4.1. Employee/Administrator Actions	60
10.4.2. IT Department/Website Security Team Actions	60
10.5. Containment and Eradication	61
10.5.1. Contain the Threat	61
10.5.2. Eradicate the Threat	61
10.6. Recovery and Communication	61
10.6.1. System Recovery	61
10.6.2. Internal Communication	61
10.6.3. External Communication	62
11. Incident Response Strategy for Doxxing of an Organizational Member	62
11.1. Purpose	62
11.2. Scope	62
11.3. Incident Detection	62
11.3.1. Indicators of Doxxing	62
11.3.2. Doxxing Early Warning System	63
11.4. Immediate Response Steps	63
11.4.1. Executive/Leadership Actions	63
11.4.2. Security/IT Team Actions	63
11.5. Containment and Mitigation	64
11.5.1. Contain the Spread	64
11.5.2. Support for the Affected Individual	64
11.6. Recovery and Communication	64
11.6.1. Internal Communication	64
11.6.2. External Communication	64
12. Self-Care Recommendations for After Being Doxxed	64
12.1. Emotional Self-Care	65
12.1.1. Acknowledge Your Feelings	65
12.1.2. Practice Stress-Reduction Techniques	65
12.1.3. Establish Boundaries	65
12.2. Practical Self-Care	65
12.2.1. Address Security Concerns	65



12.2.2. Protect Personal Information	65
12.3. Legal and Administrative Steps	66
12.3.1. Report the Incident	66
12.3.2. Document the Incident	66
12.4. Long-Term Self-Care	66
12.4.1. Build a Support Network	66
12.4.2. Engage in Positive Activities	66
12.5. Professional Help	66
12.5.1. Seek Therapy or Counseling	66
12.5.2. Legal Consultation	66
References and Resources:	68

1. Purpose and Scope

The purpose of this Digital Safety Policy is to protect the organization's digital assets, safeguard sensitive information, and ensure the safety and security of all stakeholders who interact with the organization's digital platforms. The Digital Safety Policy is meant to be a living document that evolves with the needs of the organization. It is designed to be implemented at the beginning of the onboarding process, and as a reference material for the continued development of an organization's digital growth.

This policy applies to all employees, contractors, volunteers, and third-party vendors who have access to the organization's digital systems, data, and online platforms. It covers the use of all digital devices, networks, software, and information systems owned or operated by the organization.

2. Team Members

Please review this list of team members who have key responsibilities within the digital safety plan. Critical roles include the Primary Account Holder, Secondary Account Holder, Super Admin, Admin, Incident Response Leads, and Record Keeper. Depending on the size of your organization and the number of softwares used, these roles may have more than one person involved.

[Organization Employee Directory]

Description of Critical Roles:



Primary Account Holder - An individual who is responsible for the application set up and monitoring of all the users of that application. They will have the ability to modify settings and the number of users.

Secondary Account Holder - An individual who has access to an application and has permission from the Primary Account Holder to use the application.

Super Admin - An individual who has the ability to add and remove any users from any system used by the organization, and has access control to all electronic devices used by the organization. This role is typically held by a senior leader of the organization.

Admin - An individual who has the same abilities as the Super Admin, and can act on their behalf. This role is responsible for the onboarding and offboarding tasks for all staff members regarding access to technology and systems within the organization.

Incident Response Lead - An Individual who will be notified in the event of any digital safety related incidents at the organization. The incident response lead is trained in reactive care strategies for the individual staff members and the organization itself. It is ideal that each organization has 2 or more Incident Response Leads.

Record Keeper - An individual who works with the admin team and Incident Response Lead to collect data on any incidents and stores it in an organized system.

3. Digital Accounts Tracking

Organizational Policy for Digital Account Tracking Tools

3.1. Purpose and Scope

The purpose of this policy is to establish guidelines for the use of digital account tracking tools within the organization. These tools help manage and monitor online accounts, ensuring that access to organizational systems is secure and that account activity is properly tracked and managed.

This policy applies to all employees, contractors, and third-party vendors who access the organization's systems, networks, or data. It covers the selection, use, and management of digital account tracking tools for all digital accounts used within the organization.

3.2. Policy Statement



All employees must use approved digital account tracking tools to manage and monitor their accounts related to organizational systems and data. These tools are essential for maintaining security, auditing access, and ensuring compliance with organizational policies.

3.3. Digital Account Tracking Tool Selection

3.3.1. Approved Tools

- The IT department is responsible for selecting and approving digital account tracking tools for organizational use. Approved tools must meet the following criteria:
 - **Security:** The tool must offer robust security features, including encryption, two-factor authentication (2FA), and secure access controls.
 - **Comprehensive Tracking:** The tool must provide comprehensive tracking of account creation, usage, and access logs.
 - **Reporting Capabilities:** The tool must offer detailed reporting features that allow for regular audits and reviews of account activity.
 - User Management: The tool must support role-based access controls, enabling the assignment of appropriate permissions to users based on their job responsibilities.

3.3.2. Prohibited Tools

• The use of unapproved or personal account tracking tools is strictly prohibited for managing organizational accounts. Only tools vetted and approved by the IT department may be used. If an employee is unsure if a tool or software is permitted, they are to submit a request to the administrative department for review and approval.

3.4. Account Management Practices

3.4.1. Account Creation

- **Authorization:** All new digital accounts must be created following approval from the relevant department head or IT department. The creation of new accounts must be logged and tracked using the approved digital account tracking tool.
- Note for organization: what is the master email and who has access to it (Super Admin?). If your organization has less than 5 members, please ensure that at least two members have access to the Super Admin status.
- Account Information: Account information, including usernames, roles, and permissions, must be accurately recorded in the tracking tool.

3.4.2. Account Monitoring

• **Regular Monitoring:** The IT department must regularly monitor account activity to detect any unauthorized access, unusual behavior, or potential security risks.



• Automated Alerts: The account tracking tool should be configured to send automated alerts in case of suspicious activity, such as multiple failed login attempts, access from unfamiliar IP addresses, or login outside of normal business hours.

3.4.3. Account Reviews

- **Periodic Audits:** Periodic audits of all digital accounts must be conducted to ensure that access permissions are appropriate and that no unauthorized accounts exist.
- **Deactivation of Inactive Accounts:** Accounts that have not been used for a defined period (e.g., 180 days) should be reviewed and potentially deactivated to reduce security risks. It is recommended that the administrative department schedules an audit review check of all accounts every 3 months (or once a quarter).

3.5. Training and Support

3.5.1. Employee Training

- **Initial Training:** All employees must complete training on the use of approved digital accounts upon joining the organization or when new tools are implemented.
- **Ongoing Training:** The organization will provide ongoing training and resources to help employees effectively use digital account tracking tools and stay informed about best practices in account management and security.

3.5.2. IT Support

• The IT department will provide support for setting up and using the approved account tracking tools, including troubleshooting common issues and answering security-related questions. If your organization does not have the capacity for an IT department, please ensure you are securing incident response support through outside help (see Section 5 for details).

3.6. Data Security

3.6.1. Protecting Digital Assets

- Internal Personnel Information: All employees must keep internal personnel information (e.g. staff, contractors, volunteers) confidential and stored securely. This information should be stored in an encrypted database with controlled access. The Human Resources team is responsible for keeping this data secure. Always obtain explicit consent before recording or sharing personal information, ensuring compliance with privacy regulations and ethical standards.
- **Regular Backups**: Digital assets should be backed up in either a cloud-based storage or hardware storage to ensure data availability in case of failure or cyber incidents. The IT team is responsible for managing the backups to ensure that backups are automated or manually updated on a regular basis.



- **Financial Records and Critical Records**: Financial information should be kept encrypted and/or password protected with limited access (only authorized personnel)
- For more information on protecting and managing assets can be found here: <u>https://islamicfamily.notion.site/IslamicFamily-Cybersecurity-Policy-</u> <u>c57681d4bf90456b9b7eb013a483fbb5</u>

4. Digital Identity

Organizational Policy for Protecting Employee Digital Identities

4.1. Purpose

The purpose of this policy is to establish guidelines and best practices for protecting the digital identities of employees within the organization. This policy aims to safeguard employees from identity theft, cyberattacks, and unauthorized use of their personal and professional digital identities.

4.2. Scope

This policy applies to all employees, contractors, and third-party vendors who interact with the organization's systems, networks, or data. It covers the protection of digital identities across all platforms and devices used in the course of conducting organizational business.

4.3. Policy Statement

The organization is committed to protecting the digital identities of its employees. All employees must follow the established guidelines to ensure that their digital identities, both personal and professional, are secure and that organizational resources are not compromised.

4.4. Digital Identity Protection Practices

4.4.1. Account Security

- Employees must create strong, unique passwords for all accounts related to organizational work, adhering to the organization's password complexity requirements. Recommendations include:
 - A length of 12-24 characters or more
 - A combination of uppercase letters, lowercase letters, numbers and special characters



- Does not use personal information, dictionary words or predictable patterns. For example, avoid using your name, birthday or series of numbers in order because 'Alex12345' or 'Password1' can be easily guessed.
- Consider using a passphrase that is easy to remember but hard for others to guess. For example, the phrase "My snake loves to dance at night" could be transformed into a stronger password with numbers and special characters to make "My \$nake loves 2 dAnce @ n1ght".
- Do not reuse a password across multiple accounts

For more information on choosing strong passwords:

https://www.keepersecurity.com/blog/2024/06/24/how-many-characters-should-my-password-be/

- **Multi-Factor Authentication (MFA):** Employees must enable multi-factor authentication (MFA) on all accounts that support it, particularly those used to access organizational systems or sensitive data. This provides an additional layer of security that verifies your identity when logging into an account. This involves using at least one of the following authentication factors in addition to your password:
 - SMS (text message): Add your phone number as a security method. You will
 receive an SMS text message with a one-time code to verify your identity.
 Beware that this method has security limitations, including the risk of
 unencrypted messages being intercepted and susceptibility to SIM-swapping
 attacks. However, SMS MFA is still a valuable security option and significantly
 improves account protection compared to relying solely on a password
 - Third-party authenticator app: An authenticator app can be downloaded on your mobile device. This either generates a one time code required after entering your password or a push notification to approve login. Examples include <u>Google</u> <u>Authenticator</u>, <u>Microsoft Authenticator</u> or <u>Duo</u>).
 - Security keys/Hardware tokens: A physical device that your system must detect to verify your identity. They come in various forms, such as USB drives, key fobs, or NFC-enabled devices, and work by generating time-sensitive codes, performing cryptographic operations, or connecting directly to a computer or smartphone. For example, <u>Google's Titan Security Key</u> is a physical USB security key that can either be inserted into your computer or connected via NFC.
 - Some accounts provide recovery codes that serve as a backup when your device is unavailable for multi-factor authentication (MFA). These codes are typically generated at the end of the MFA setup process. It is highly recommended to store them securely in a place that remains accessible even if your device is lost or unavailable. A secure option is to save them in a trusted password manager for easy retrieval when needed.
 - Your organization has selected (this option) for your digital safety purposes. The Admin/Tech Lead is responsible for providing you with set up and training for this procedure. Please contact them with any questions regarding the set up or maintenance of the process.



- **Password Management:** Employees are required to use an approved password manager to store and manage passwords securely, reducing the risk of password reuse and breaches. Some examples of password managers are <u>Google Password Manager</u>, <u>Bitwarden, 1Password, DashLane</u>, and <u>Keeper</u>
 - Your organization has selected (this option) for your digital safety purposes. The Admin/Tech Lead is responsible for providing you with set up and training for this procedure. Please contact them with any questions regarding the set up or maintenance of the process.

You can use a password manager to:

- Create and save strong, unique passwords to your account so you don't have to remember them.
- Protect all your saved passwords with built-in security.
- Automatically fill in passwords on sites and apps.
- Employees must ensure that the password manager is protected through multi-factor authentication (MFA) and/or the master password meets the organization's password complexity requirements and is not reused across other accounts. Also be sure to update passwords on regular basis (eg. every 3 months). Some password managers have a feature to set up reminders, otherwise schedule reminders manually in your calendar in collaboration with your IT Team.

Information on passwords and MFA was found from the Social Media Security & Privacy Checklists resource linked in this article:

Kozinski, K. & Kapur, N. (2020, February 27). *How to Dox Yourself on the Internet*. New York Times. <u>https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954</u>

4.4.2. Email and Communication Security

- **Phishing Awareness:** Employees must complete regular training on recognizing and avoiding phishing attempts. Phishing is a form of **social engineering**, where attackers manipulate or deceive individuals into revealing confidential information. This often involves creating a false sense of urgency, such as claiming an account will be locked unless the victim clicks on a malicious link. Employees should be trained to identify red flags and report suspicious emails or communications to the IT department immediately. To strengthen awareness, organizations should conduct ongoing phishing simulation tests monthly to test employees' responses in real-world scenarios. These simulations can highlight areas where additional training is needed.
 - Phishing examples:
 - A phishing email may impersonate your bank, asking you to click on a link to verify your account due to "suspicious activity" or to accept an etransfer. The link leads to a fraudulent website designed to steal your login credentials. Legitimate banking communications will typically be sent to the personal email address you've registered with the bank, not



your work email. To stay safe, always log in directly through your bank's official website or app rather than clicking on links in emails.

INTERAC e-Transfer: government sent you 2000.00 (CAD)

You ⊗	
Interac e-Transfer	(
Hello, ##EMAIL##	
Canada Revenue Agency se	nt you funds.
Deposit Your Money:	
	Select your financial institution
What if you could deposit tra	nsfers without answering any questions? Sign up for Autodenosi
in your online banking - a saf	e and convenient way to receive funds straight to your bank
, .	

Hrynchuk, S. (2020, August 12). *E-Mail Money Transfer*. Scam Detector. <u>https://www.scam-detector.com/article/e-mail-money-transfer/</u>

You might receive an email claiming to be from a shipping company like UPS, FedEx, or DHL, stating that a package couldn't be delivered. The email often includes a link to "reschedule delivery" or pay a fee, but the sender's email address will likely not match the shipping company's domain. If you're not expecting a delivery or the email is sent to your work address for a personal purchase, it's likely a scam. Always verify directly with the shipping company through their official website or app.



Subject:UPS Delivery Notification Date:Tue, 15 Mar 2016 22:10:20 +0100 From:UPS <atlas:@omantel.net.om>

UPS Privacy Notice | Contact UPS

Dear Customer,	
Your Parcel has experienced an exception. This Could be due to several reasons inc address and other exceptions.	luding :invalid address, no authorized person at the
Action Required:	
Please click link below to sign in to your UPS account to print the invoice and tracking	g number to pick up the package at ups store
Click here https://www.ups.com/	
Not registered with My UPS?	
With My UPS, everything you need to ship is available in one place. My UPS keeps y format. As a My UPS user, you select the tools that will help you work most efficiently to make My UPS work for you, please visit <u>Getting Started</u> .	our shipping data in a customizable, easy-to-use and save them all on same page. To learn more ways
2015 United Parcel Service of America, Inc. UPS, the UPS brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.	
All trademarks, trade names, or service marks that appear in connection with UPS's services are the property of their respective owners.	
Please do not reply directly to this e-mail. UPS will not receive any reply message. For more information on UPS's privacy practices, refer to the UPS Privacy Notice. For questions or comments, wite Contact UPS.	
This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.	

UPS. (2025). Protect Yourself From Fraud and Scams. UPS.

https://www.ups.com/ca/en/support/shipping-support/legal-terms-conditions/fight-fraud.page

Phishers might send an email with an image or attachment labeled as an invoice. The email claims that you must contact a phone number to "cancel" the transaction. Once you call, they'll attempt to extract personal or financial information. If you were not expecting an invoice or the document lacks legitimate sender details, such as an official email address or a specific contact person, it's almost certainly fraudulent. Avoid engaging and report the email to your IT team.



Site Admin. (2022, September 26). *Fake Invoice Phishing Scams*. Information Technology Lawrence Berkeley National Laboratory. <u>https://it.lbl.gov/fake-invoice-phishing-scams/</u>

- How to spot a phishing email:
 - Check the sender's email address: Phishing emails often come from addresses designed to look legitimate but contain small typos or unusual domains (e.g., support@paypa1.com instead of support@paypal.com). Always verify the sender's email carefully. Hint: check the company's website to be sure!
 - Look for Spelling and Grammar Errors: Poor grammar, spelling mistakes, or awkward phrasing are common in phishing emails. Legitimate organizations typically ensure their communications are polished and professional.
 - Hover Over Links Without Clicking: Before clicking any links, hover your cursor over them to see the actual URL. If the link doesn't match the organization's official website or appears suspicious (e.g., a random string of characters or an unfamiliar domain), it's likely phishing.



- Avoid Unexpected Attachments: Be cautious of unexpected attachments, especially in unusual formats like .exe, .zip, or .scr, as these files often contain malware. Only open attachments from trusted sources.
- Look for Generic Greetings: Phishing emails frequently use generic greetings like "Dear Customer" or "Hello User" instead of addressing you by name. Trusted organizations typically personalize emails to address you directly
- Beware of Urgent or Threatening Language: Many phishing emails create a false sense of urgency or fear to manipulate you into acting quickly. Common phrases include "Your account will be locked in 24 hours" or "Immediate action required!" Always take a moment to verify before reacting.
- Look for an email signature: Legitimate organizations include professional email signatures with relevant contact information and branding, such as logos. If an email lacks these elements or looks unprofessional, it could be fraudulent.
- Avoid using QR codes from unfamiliar or suspicious websites.

For more examples on fake emails and what signs to look out for, check Government of Canada's Get Cyber Safe Resources Website:

https://www.getcybersafe.gc.ca/en/resources/real-examples-fake-emails

- Secure Communication Channels: Employees should use only approved and secure communication channels (e.g., encrypted email, secure messaging apps) for sharing sensitive information.
 - Secure Messaging Apps (e.g., Signal, WhatsApp): For private communication, use encrypted messaging apps like Signal or WhatsApp. If you're using WhatsApp, enable two-factor authentication (2FA) for added security. Also, ensure that your app is always updated to the latest version to benefit from the latest security patches.
 - Avoid Unsecured Platforms (e.g., SMS, social media, or personal email): Never share sensitive organizational information over unsecured channels such as SMS, Facebook Messenger, or personal email accounts, as these do not offer sufficient encryption or protection against interception.
 - Using File Sharing Services (e.g., Google Drive with encryption, Dropbox with two-factor authentication): When sharing sensitive files, use services that support encryption and strong access control. For Google Drive, ensure that the file is shared with only authorized individuals and enable the option to restrict downloading or sharing. For Dropbox, activate two-factor authentication to protect your account.
 - Encrypted Email (e.g., Gmail or Outlook with encryption): Always use encrypted email services or enable encryption features when sending sensitive information. Gmail automatically encrypts the email in transit using transport-layer security (TLS). If you're using Outlook, ensure that the message is encrypted by selecting the "Encrypt" option before sending.



- Email Signature Safety: Personal information in email signatures should be kept minimal. Avoid including details like personal phone numbers, addresses, or other sensitive information. This may be extended to include full names or hyperlinks to third party sites.
 - Company needs to set standard for the degree of confidentiality needed for each employee, and what they are consenting to share about themselves publicly.
- **Vishing**: Vishing, or voice-phishing, is a social engineering threat where attackers use phone calls or voice communication to manipulate individuals into revealing sensitive information. This often involves techniques such as caller ID spoofing, fake phone numbers, or voice cloning. Attackers may impersonate trusted sources like family members, friends, employers or service providers.
 - Vishing Examples:
 - Bank fraud: Attackers pose as bank representatives and claim there has been fraudulent activity on your account. They'll ask for personal information (e.g., account details, PINs etc.) to secure your account or ask you to transfer your funds to another account. Always verify bank fraud alerts through your mobile banking app, email or local banking centre.
 - Government impersonation: Attackers impersonate government officials (e.g., CRA) demanding personal and financial information to process a tax refund, verify your identity or make a payment. Official government agencies will not contact you for this information over the phone, they send mailed letters or request you to bring in documents in-person to a government office.
 - Signs of Vishing:
 - Poor audio quality or background noise
 - Unsolicited requests for sensitive information about yourself or someone you know
 - A sense of urgency or threatening language to coerce you into responding quickly without thinking
 - An urgent text from family/collegaure from a new number
 - If unsure, hang up and call your IT team/trusted colleague directly to confirm requested information or action before moving forward.

Check these resources to learn more about vishing:

https://www.getcybersafe.gc.ca/en/blogs/what-vishing https://www.cyber.gc.ca/en/what-voicephishing-vishing-itsap00102 https://us.norton.com/blog/online-scams/vishing https://www.comparitech.com/blog/information-security/what-is-vishing-how-to-avoid/

4.4.3. Social Media and Public Profiles

• **Privacy Settings:** Employees must review and adjust the privacy settings on their social media and public profiles to limit the exposure of personal information. Professional profiles (e.g., LinkedIn) should be kept up-to-date with a focus on career-related content, if employees consent to do so and it is safe for them to disclose that information online.



- Company-specific privacy policy should be included here. Decide on the degree of which privacy will be kept, with consent from each employee.
- **Social Media Conduct:** Employees are advised to exercise caution when sharing personal or professional information on social media. Posts should not disclose confidential organizational information or personal details that could be exploited by malicious actors.
- For Organizations: Insert link to consent form for social media use here
- Avoid Linking Accounts: Employees should avoid linking personal accounts (e.g., personal email, social media) with work-related accounts to minimize the risk of cross-platform breaches.

Below are privacy setting recommendations for Instagram, WhatsApp, LinkedIn, BlueSky and TikTok. Please note that screenshots of instructions were taken as of February 2025.

Instagram Security & Privacy Settings

Updating Your Password to a Strong and Unique One:

- 1. Go to your **Profile Page**.
- 2. Tap the **Menu Icon** (\equiv) in the top right.
- 3. Select Account Center > Password & Security.
- 4. Tap Change Password and select the account you want to update.
- 5. Enter a new, strong password and confirm the change.

Share a nota posts	€ ⊕ (Ξ) Followers following	Settings and activity Q. Search Your account On Meto	X 03 Meta Accounts Center Manage your connected experiences and account settings across Meta technologies like Facebook, instagram and Meta Horizon, Learn more	← Password and security Login & recovery Manage your passwords, login preferences and recovery methods.	Change password Choose an account to make changes.
Edit profile	Share profile	Password, security, personal details, ad preferences	Profiles	Change password	j⊚ instagram
Discover people		Manage your connected experiences and account settings across Meta technologies. Learn more		Two-factor authentication >	
		How you use Instagram	Connected experiences	Saved login Ø >	
Find more people to follow		□ Saved >	 A Sharing across profiles →) Logging in with accounts 	Security checks Review security issues by running checks across apps, devices and emails sent.	
See all		Your activity >	Account settings	Where you're logged in >	
m	Ŕ	♦ Notifications >	Password and security	Login alerts >	
ш	<u>d</u>	① Time management >	Personal details	Recent emails (C) >	
			Fa Your information and permissions >	Security Checkup 🕥 >	
		Account privacy Public >	📢 Ad preferences >		
Ω Ω	Ð D	Class Friends	🖬 Meta Pay >		

Setting Up Two-Factor Authentication (2FA):

- 1. Go to your **Profile Page**.
- 2. Tap the **Menu Icon** (\equiv) in the top right.



- 3. Select Account Center > Password & Security > Two-Factor Authentication.
- 4. Choose the account you want to secure.
- 5. Select a security method (e.g., Authentication App, SMS, or WhatsApp) and follow the on-screen instructions.

	(
6	⊕(≡)	← Settings and activity	X Ø Meta
Share a note	7	O Search	Accounts Center
posts followers follo	wing	Veus essenat	Manage your connected experiences and account settings across Meta technologies like Facebook,
		Accounts Contor	Instagram and Meta Horizon. Learn more
Edit profile Share profile	e (*2	Password, security, personal details, ad preferences	Profiles
Discover people		Manage your connected experiences and account settings across	
,		Meta technologies. Learn more	Connected experiences
		How you use Instagram	♣ Sharing across profiles >
Find more people to follow		Saved >	→ → Logging in with accounts >
See all		Archive >	
Jeean		Your activity >	Account settings
	3	♦ Notifications	Password and security >
		① Time management >	Personal details >
			Your information and permissions >
		Account privacy Public >	Ad preferences >
	0	A class Friends	🖨 Meta Pay >
←		← Done	÷
Password and security		Two-factor authentication	Instagram
Login & recovery		Choose an account to set up two-factor authentication.	account
methods.			Two-factor authentication protects your account by requiring an additional code when you log in on
Change password			a device we don't recognize. Learn more
Two-factor authentication	>		
Saved login			Authentication app Recommended • We'll recommend an app to download if you don't have one
Security checks			It will generate a code you'll enter when you log in.
Review security issues by running checks acro devices and emails sent.			SMS or WhatsApp
Where you're logged in			We'll send a code to the mobile number O you choose.
where you relogged in			
Login alerts			
Recent emails			
Recent emails Security Checkup			
Recent emails Security Checkup			Next
Recent emails Security Checkup			Next

Managing Your Data & Activity Outside Meta:

- 1. Go to your **Profile Page**.
- 2. Tap the **Menu Icon** (\equiv) in the top right.
- 3. Select Account Center > Your Information & Permissions > Your Activity Off Meta Technologies.
- 4. Clear Previous Activity: Remove data linked to external sites and apps.
- 5. **Manage Future Activity:** Select **Disconnect Future Activity** to prevent tracking from external sources.



	← Settings and activity	Х ФМ	eta	÷		÷
Stare a note	Q Search	Accounts	s Center	Your informatio	on and	Your activity off Meta
posts followers following	Your account	Manage your connected e settings across Meta tech	experiences and account nologies like Facebook,	permissions		technologies
		Instagram and Meta F	Horizon. Learn more	Download your informa	ition >	Your activity off Meta technologies includes information that businesses and organizations
Edit profile Share profile	Accounts Center Accounts Center Password, security, personal details, ad Accounts Center	Profiles		Transfer a copy of your	information >	share with us about your interactions with them such as visiting their apps or websites.
Discover people See all	preferences					A Learn more shout activity off
	Meta technologies. Learn more	Connected experience	es.	Search history		Meta technologies
	How you use Instagram	O charles and		View, download or transfer yo on our apps.		What you can do
	Saved >	C, Sharing across pro	ornes >		E.	You can control or disconnect the information
Find more people to follow	Archive >	→ Logging in with ac	counts >	Your activity off Meta t	echnologies >	businesses send to meta.
See all	A Your activity	Account settings		Specific ad partners		() Recent activity You have no available activity to >
			urity ,	Upload contacts		
i i i i i i i i i i i i i i i i i i i	Notifications		unty 2			Disconnect specific activity
	Time management	Personal details		influence your experiences.		
		Fa Your information a	and permissions 🖉 >			Clear previous activity >
	Account privacy Public >	Ad preferences				C Manage future activity >
	Class Estanda	Meta Pay				
← Clear previous a Your activity history will be your account. Clear previous activity @ Instagram	te disconnected from → te di	Doff Meta exchnologies includes sesses and organizations ops or websites. ubout activity off logies onnect the information ta. alable activity to te. wific activity wific activity activity activity	← Manage future Used for 1 account > Concert future activity Well concert future activity Used in account > Concert future activity The spont current experie Used in the spont current experies Used in the spont current experime experies Used in the spont current experies	Activity which that tations send us with them. which we will also with fure activity, we'll also which there activity, we'll also	 What you shoul When you discome supported to you in account of you in account of you in account of the businesses are many account. It may take account of the a	Id know try our thoices will be accounte guite will able to the second the second second second second second the second second second second second the second second second second second second the second second second second second second second the second

Removing Uploaded Contacts:

- 1. Go to your **Profile Page**.
- 2. Tap the **Menu Icon** (\equiv) in the top right.
- 3. Select Account Center > Your Information & Permissions > Upload Contacts.
- 4. Toggle **Connect Contacts** off to stop Instagram from accessing and storing your contacts.



Share a nota posts	6 D D	Settings and activity Q Search Your account 00 Meto	X COMeto Accounts Center Manage your connected experiences and account settings across their technologies like Pacebook, Instagram and Meta Horizon. Learn more	← Your information and permissions	← Contacts syncing Connect contacts ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Edit profile Discover people	Share profile 🛃	Accounts Center	Profiles >	Transfer a copy of your information >	contacts to follow. Disconnect anytime to stop syncing contacts from this device. This will not delete your previously synced contacts, which you can delete in Settings on Instagram.com. Learn more
		Meta technologies. Learn more How you use Instagram	Connected experiences	View, download or transfer your information and activity on our apps.	
Find more people to follow		□ Saved > ○ Archive >	Logging in with accounts	Your activity off Meta technologies > Specific ad partners >	
	Ø	✓ Your activity > ▲ Notifications >	Password and security	Upload contacts >	
		Who can see your content	E Your information and permissions		
<u>ଜ</u> ଦ	+ • ·	Account privacy Public >	SU Ad preferences >		

Temporarily Limiting Interactions to Avoid Harassment:

If you're experiencing unwanted interactions, you can temporarily limit engagement from certain users.

- 1. Go to your Profile Page.
- 2. Tap the **Menu Icon** (\equiv) in the top right.
- 3. Select Limit Interactions.
- 4. Choose what to limit (e.g., comments, messages).
- 5. Select who to limit (e.g., accounts that don't follow you or recent followers).
- 6. Set the **duration** (maximum of 4 weeks)





Filtering Out Offensive Words & Phrases:

- 1. Go to your **Profile Page**.
- 2. Tap the **Menu Icon** (\equiv) in the top right.
- 3. Select Hidden Words.
- 4. Enable **Hide Offensive Comments & Message Requests** to automatically filter harmful content.
- 5. Create a **Custom Words List** by adding specific words, phrases, or emojis you don't want to see then **Hide comments & Message requests** for those words
 - Check here for a full list of bad words that are already banned by Google <u>https://web.archive.org/web/20240418094602/https://www.freewebheaders.com/f</u> <u>ull-list-of-bad-words-banned-by-google/</u>

© ⊕(≡)				\leftarrow Add words or phrases «
	← Settings and activity	Hidden words	← Hidden Words	
Share a note	Crossposting	Unwanted comments and message requests	Hide comments	Add words separated by commas Add
posts followers following	S Blocked	Hide comments	Comments that are potentially offensive, misleading or spam will be moved to a separate section. Anyone can see these comments, and you can unbide comments on your own nexts at anytime. Learn more	You can add multiple words, phrases and emojis. Your list can be undated anytime.
	𝔅 → Hide story and live	Comments that are potentially offensive, misleading or spam will be moved to a separate section. Anyone can see these comments, and	Advanced comment filtering	Tan to view your list
Edit profile) Share profile) (**)	How others can interact with you	you can unhide comments on your own posts at anytime. Learn more		Top to Hell your tist
Discover people See all	 Messages and story replies 	Advanced comment filtering	Even more comments that meet our criteria will automatically be hidden.	
	Tags and mentions	Even more comments that meet our criteria will automatically be hidden.	Hide message requests	
	Q Comments	Hide message requests	Message requests that may be offensive, spam or scams will be moved to the Hidden requests folder. We'll also filter notifications for these messages. This feature is not currently supported on web	
Find more people to follow	🗘 Sharing and reuse	Message requests that may be offensive, spam or scams will be moved to the Hidden requests folder. We'll also filter notifications for these messages. This feature is not currently supported on web	or Meta Quest.	
	Destricted	or Meta Quest.	custom words for messages and comments	
See all	Kestricted	Custom words for messages and comments	Manage custom words and phrases $~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~$	
n in the second se	() Limit interactions	Manage custom words and phrases $>$	Hide comments	
	Aa Hidden Words 🥿	Hide comments	Comments that contain words, phrases or emojis on your custom list and similar misspellings will be filtered out so they are only visible	
	+A Follow and invite friends	Comments that contain words, phrases or emojis on your custom list and similar misspellings will be filtered out so they are only visible	to the authors.	
	What you see	to the authors.	Hide message requests	
	☆ Favorites	Hide message requests	Message requests that contain words from your list will be hidden. This feature is not currently supported on web or Meta Quest.	

For more information on how to filter, block and report harmful content on social media, you can check here: <u>https://rainn.org/articles/how-filter-block-and-report-harmful-content-social-media</u>.

WhatsApp Security & Privacy Settings

Set Up Two-Factor Authentication (2FA):

- 1. Tap the **Menu Icon** (:) in the top right.
- 2. Go to Settings > Account > Two-Step Verification.
- 3. Tap Turn On and create a 6-digit PIN.
- 4. This PIN will be required the next time you log in with your phone number.



	-								
WhatsApp		WhatsApp	<u>ه</u> ۹ :	÷ \$	Settings	م	← .	Account	← Two-step verification
Q Ask Meta Al or Search	1		New group				0	Security notifications	
Archived		Archived	New broadcast		1		2 9	Passkeys	* * *
A Your personal messages are end-	to-end encrypted		Linked devices	©	Account Security notifications, change number			Email address	For extra security, turn on two-step verification, which will require a PIN when registering your phone
		\rightarrow	Starred messages		Privacy Block contacts, disappearing messages			Two-step verification	
				•	Avatar		L)	Change number	
				U				Request account info	
					Lists Manage people and groups		o Do	Add account	
					Chats Theme, wallpapers, chat history			Delete account	
	0		0	¢	Notifications Message, group & call tones				/
	D		•	0	Storage and data Network usage, auto-download				
کے لیے لیے لیے لیے لیے لیے لیے لیے لیے لی	Ls % unities Calls	E Ø Chats Updates	සා ද Communities Calls	⊕	App language English (device's language)				Turn on

Enable a Passkey for Added Security:

Passkeys allow you to log in securely using **Face ID**, **Fingerprint**, **or Screen Lock** instead of a PIN.

- 1. Tap the **Menu Icon** (:) in the top right.
- 2. Go to Settings > Account > Passkeys.
- 3. Tap **Create Passkey** and follow the instructions.
- 4. Your passkey will be securely stored in your password manager for future logins.

It is not recommended that you use any biological identification (e.g., Face ID, Fingerprints), for your digital devices, or for personal or workplace identification, as it poses a safety risk for yourself and those around you. Screen Locks and numerical pins are always the strongest and safest option, and cannot be unlocked without legal permission (e.g., a bench warrant) by a member of law enforcement. Face ID is also sensitive to size and shape, and is especially not recommended for those considering undergoing future physical changes or gender affirming care.



	_									
WhatsApp	@ < (i)	WhatsApp	<u>ه</u> ۹ :	÷ :	Settings	Q	÷ ,	Account	÷	Passkeys
Q Ask Meta Al or Search	1		New group		8	₹ ⊕	0	Security notifications		
Archived		Archived	New broadcast		1		2 9	Passkeys 🗲		
හා Your personal messages are end-t	o-end encrypted		Linked devices	س	Account Security notifications, change number			Email address		•
		\rightarrow	Settings		Privacy Block contacts, disappearing messages			Two-step verification		<u> </u>
				e	Avatar			Change number		Log in securely and protect your account
					Create, edit, profile photo			Request account info		Create a passkey for a secure, easy way to log into your account.
				e	Manage people and groups		0°	Add account		Log into WhatsApp with your face, fingerprint or screen lock.
					Chats Theme, wallpapers, chat history			Delete account	Б	Your passkey is stored safely in your password manager.
	0		0	¢	Notifications Message, group & call tones					
	P			0	Storage and data Network usage, auto-download					
ළ ගි දුදි Chats Updates Commu	s ጜ nities Calls	E Ø Chats Updates	<u>දස</u> Communities Calls	⊕	App language English (device's language)					Create passkey

Protect Your IP Address & Block Unknown Accounts:

- 1. Tap the **Menu Icon** (:) in the top right.
- 2. Go to **Settings > Account > Privacy > Advanced**.
- 3. Enable the following options:
 - **Block Unknown Account Messages** Prevents messages from unverified contacts.
 - Protect IP Address in Calls Hides your IP address during calls for better security.
 - **Disable Link Previews** Prevents link previews from revealing your data.



Wha	ts∆nn	ര	a (;	WhatsApp	â	Q :	← Settings Q
	isk Meta Al or Search		1	Ask Meta Al or Se	New group		
Ð	Archived		$\int $	Archived	New broadcas	st	# +
ð			crypted		Linked device	es ages	C Account Security notifications, change number
				\rightarrow	Settings		Privacy Block contacts, disappearing messages
							Avatar Create, edit, profile photo
							Lists Manage people and groups
							E Chats Theme, wallpapers, chat history
			0			0	Notifications Message, group & call tones
			Ð				O Storage and data Network usage, auto-download
Chats	ي (Q) وي Updates Comm	S unities	حم Calls	Chats Updates	دی Communities	م Calls	App language English (device's language)
← s	ettings		م	← Privacy			← Advanced
				Groups My contacts			Block unknown account messages To protect your account and improve device performance, WhatsApp will block messages from unknown accounts if they
©	Account Security notifications, cha			Live location			exceed a certain volume. Learn more Protect IP address in calls
⋳	Privacy Block contacts, disappear	ing mess	ages	Calls Silence unknown callers			To make it harder for people to infer your location, calls on this device will be securely relayed through WhatsApp servers. This will reduce call quality.
•	Avatar Create, edit, profile photo			Blocked contacts			Learn more Disable link previews
g	Lists Manage people and group			App lock Disabled			To help protect your IP address from being inferred by third-party websites, previews for the links you share in chats will no longer be generated. Learn more
E	Chats Theme, wallpapers, chat h			Allow camera effects			
¢	Notifications Message, group & call ton			Advanced			
0	Storage and data Network usage, auto-dow			Protect IP address in call:			
⊕	App language English (device's language			Privacy checkup Control your privacy and c you.			

Perform a Privacy Checkup:

- 1. Tap the **Menu Icon** (:) in the top right.
- 2. Go to Settings > Privacy > Privacy Checkup.
- 3. Adjust settings to:
 - Choose who can contact you.
 - Control your personal information visibility.
 - Add extra privacy to chats.
 - Strengthen account security and protection.



WhatsApp 🖻 ९ 🤃	WhatsApp	<u>ه</u> ۷ :	÷ 5	Settings	م	← Privacy	÷	Privacy checkup
Q Ask Meta Al or Search		New group			號 ⊕			
Archived	Archived	New broadcast				Groups My contacts		
		Linked devices	© 7	Account Security notifications, change numb		Live location		
	\rightarrow	Starred messages		Privacy Block contacts, disappearing messar	qes	Calls Silence unknown callers		Your privacy matters
			•	Avatar Create.edit.profile.photo		Blocked contacts 36		trol your privacy settings and set up WhatsApp just the way you want it.
				Lists Manage people and groups		App lock Disabled		Choose who can contact you $ ightarrow ightarrow$
						Chat lock		Control your personal info $ ightarrow$
				Chats Theme, wallpapers, chat history		Allow camera effects Use effects in the camera and video calls.		Add more privacy to your chats $ o$
0		0	¢	Notifications Message, group & call tones		Advanced	Ĝ	Add more protection to your $\qquad \rightarrow \qquad$ account
•		•	0	Storage and data Network usage, auto-download		Protect IP address in calls, Disable link previews		
E D & & C	Chats Updates	සා ද Communities Calls	⊕	App language English (device's language)		Privacy checkup Control your privacy and choose the right settings for you.		



LinkedIn Security & Privacy Settings

Update Your Password to a Strong and Unique One:

- 1. Tap your **Profile Picture**.
- 2. Go to Settings > Sign In & Security > Change Password.
- 3. Enter your current password, then create a strong, unique password that follows best security practices.

Search		<i>←</i>		8	← Change password ?
Like Comment Repost Send		Settings	Account access		Create a new password that is at least 8 characters long.
Department of Education : 91,053 followers Promoted			Email addresses		What makes a strong password?
Are you a teacher looking for your next adventure? Swap Victoria, British Columbia for Victoria, Australia see more		Account preferences	Phone numbers		Type your current password *
	+ Experience	🔒 Sign in & security 🧲	Change password		- ·
46	profile viewers		Passkeys		lype your new password *
107	7 post impressions	 Visibility 	Where you're signed in		Retype your new password *
Teach in Australia	a	Data privacy	Devices that remember your password		Demine all durings to sign in with new passward
Enjoy our nature	uzzle games sture	🗔 Advertising data	Two-step verification		Require an devices to sign in with new password
Sa Sa	aved posts		App lock		
TEACH THE PUTURE	roups	A Notifications			Forgot Password
		1			
Teach in Victoria, Australia Learn more	Reactivate Premium: 0%	Help Center			
RRO 79 1 comment • 2 renosts	off	Professional Community Policies			
	Settings	Privacy Policy			
Home Video My Network Netifications Jobs		Accessibility			

Set Up Two-Factor Authentication (2FA):

- 1. Tap your Profile Picture
- 2. Select Settings > Sign In & Security > Two-Step Verification.
- 3. Follow the on-screen instructions to enable 2FA using an authentication app or phone number.





Review Active Sessions & Sign Out of Unrecognized Devices:

Regularly check where your account is logged in to ensure no unauthorized access.

- 1. Tap your **Profile Picture**.
- 2. Navigate to Settings > Sign In & Security > Where You're Signed In.
- 3. Review the list of active sessions.
- 4. If you see any unfamiliar locations or devices, select **End Session** to log out immediately





Bluesky Security & Privacy Settings

Update Your Password to a Strong and Unique One:

- 1. Open Bluesky and Tap the **Menu Icon** (≡) in the top left.
- 2. Select Settings (۞) > Account > Password
- 3. Follow the on-screen instructions to change password

≡₩		← Settings		← Ac	count			
Following				🗹 Em	ail			
(a) vvv.commondreams.org	0 followers · 1 following			Øv	erify your			
🖵 580 🛱 4.5K 🗢 25.4K 🚥				~				
Nature's masterpiece # @nature-u 1d Perfect shot!	Q Search			Ch:	ange email			
🖄: Steve Woods Photography	🔒 Home	Add another account		🖨 Birt	thday	•		
	💬 Chat	8 Account		🔒 Pas	ssword 🥝	<	-	
1	\square Notifications	Privacy and security		@ На	ndle			
	# Feeds	🕐 Moderation		🕞 Exp	oort my da			
	°⊒ Lists	Content and media						
	A	Appearance						
	Profile	Accessibility						
	Settings	\delta Languages						
□ 384 🛱 1.7K 🔍 22.2K 🕜		Help						
A ⊕ A ●	© Feedback Help		0	A	Q	Ð	Q	0

Setting Up Two-Factor Authentication (2FA):

- 1. Open Bluesky and tap the **Menu Icon** (≡) in the top left.
- 2. Select Settings (Q) > Privacy and security >
- 3. Enable Two-factor authentication(2FA) and follow on screen instructions



= ¥ #		← Settings		← F	Privacy and	Security		
Siscover Following				0	Two-factor a	uthenticatio	in (2FA)	Enable
© 580 ♯ 4.5K ♡ 25.4K ····	0 followers · 1 following			, حن	App passwor	ds		
Nature's masterpiece 🏶 @nature-u 1d	Q Search			<i>©</i>	Logged-out v	isibility		
The store woods Photography	A Home	2+ Add another account] د ا	Discourage app account to logo	os from show jed-out user show your r	ring my s vrofile and n	oete to
	0	0		i t	ogged-out use his request. Th	rs. Other app is does not i	is may not h nake your a	ionor ccount
4	💬 Chat	Account			orivate.			
	Q Notifications	A Privacy and security	>	Ŷ N T	lote: Bluesky is his setting only	an open and limits the vi	I public net sibility of yo	work. sur
	# Feeds	🕐 Moderation		c 0 c	ontent on the E ther apps may ontent may stil	ut users - outer apps may not notion stst. This does not make your account ssky is an open and public network, ig ony limits the visibility of your the Bluesky app and website, and s may not respect this setting. Your ay still be shown to logged-out users pps and websites.		
-		Content and media		b	y other apps a	nd websites. ut what is nu		work. sur , and Your it users isky.
0	Cists							
	Profile							
	🕸 Settings 🧲	Accessibility						
		🕲 Languages						
▲ 384 \$1.7K Q 22.2K		Help						
n q 💬 🗘 🍥	D Feedback Help	♠ Q ഈ ₽	0	A	Q	Ô	Q	0

Moderate Content on Your Feed:

- 1. Open Bluesky and tap the **Menu Icon** (≡) in the top left.
- 2. Select **Settings** (\bigcirc) > **Moderation**
- 3. Adjust moderation settings to your preference to mute and filter certain words
 - Check here for a full list of bad words that are already banned by Google <u>https://web.archive.org/web/20240418094602/https://www.freewebheaders.com/f</u> <u>ull-list-of-bad-words-banned-by-google/</u>

Image: bit interaction Image: bit int					
Networks Following Image: Status	≡ ₩ #		← Settings	← Moderation	
Image: Store Woods Photography	Riscover Following			Moderation tools	
Stor 4.45K Q 25.4K Material store Q Search Store Woods Photography Home Chat Add another account Chat Account Chat Account Notifications Feeds E Lists Content filters Profile Appearance Settings Settings Terms of Service Fredskitt Profile Settings Profile Settings Predeskitt Profile Settings Predeskitt Profile Settings Profile Settings Predeskitt Profile Settings Predeskitt Settings Profile Settings Predeskitt Settings Profile Settings Predeskitt Predeskitt Predeskitt Profile Settings Profile Settings Predeskitt Predeskitt Predeskitt Predeskitt Predeskitt Profile Predeskitt Predeskitt <	www.commondreams.org		@	Interaction settings	
Nature's masteriores @ @nature-u1d Q. Search Image: Steve Woods Photography Image: Help Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography <t< th=""><th></th><th>0 tollowers · 1 tollowing</th><th></th><th>√ Muted words & tags</th><th></th></t<>		0 tollowers · 1 tollowing		√ Muted words & tags	
Image: Steve Woods Photography Image: Add another account Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Woods Photography Image: Steve Wood	Nature's masterpiece # @nature-u 1d Perfect shot!	Q Search		路 Moderation lists	
Privacy and security > Notifications # # Feeds := Lists © Profile © Settings * Terms of Service * Terms of Service * Peedsack * Peedback * Peedback * Peedback	🐯: Steve Woods Photography	n Home	Add another account	옷 Muted accounts	
 A Notifications # Feeds E Lists Profile Settings ← Terms of Service Terms of Service Predback Help Predback Help Content filters Cont		💬 Chat	Account	Ø Blocked accounts	
# Feeds # Feeds Imable adult content Disabled Imable adult content Disabled Imable adult content Disabled Imable adult content Imable adult content Disabled Imable adult content Disabled Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable adult content Imable		Q Notifications	Privacy and security	Content filters	
Image: Settings Image: Settings <td< th=""><th></th><th># Feeds</th><th>🖑 Moderation 🧹</th><th>Enable adult content Disat</th><th>pled 💽</th></td<>		# Feeds	🖑 Moderation 🧹	Enable adult content Disat	pled 💽
 Profile Settings Constraints Settings Constraints Constraints	Ø	\$⊒ Lists	Content and media	Non-sexual Nudity	
Image: Settings Image: Settings Image: Settings Advanced Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Settings Image: Seti		Profile		Show Warn	
Image: Constrained of the constraint of the const	~	Settings	🕲 Languages	Advanced	
A Q D G Feedback Help A O Feedback Help A O C D C C C C C C C C C C C C C C C C C			(?) Help	Bluesky Moderation Servic	e
		D Feedback Help		Official Bluesky moderation ser	vice,

Facebook Security & Privacy Settings



Updating Your Password to a Strong and Unique One:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Tap See more in Account Center > Password & Security.
- 4. Tap Change Password and select the account you want to update.
- 5. Enter a new, strong password and confirm the change



Setting Up Two-Factor Authentication (2FA):

- 1. Open Facebook and tap the Menu Icon (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Tap See more in Account Center > Password & Security > Two-Factor Authentication.



- 4. Choose the account you want to secure.
- 5. Select a security method (e.g., Authentication App, SMS or WhatsApp, Security keys) and follow the on-screen instructions.

Menu \longrightarrow 🕸 Q	< Settings & privacy Q	014-tr
ය 🖓 ස ᡐ 🗘 =	Search settings	
7		Accounts Center
Create new profile or Page Switch between profiles with one	O Meto Accounts Center Manage your connected experiences and account settings across Meta technologies.	Manage your connected experiences and account settings across Meta technologies like Facebook, Instagram and Meta Horizon. Learn more
login.	Personal details Password and security	Profiles
C Memories	Ad preferences	
Saved	Verification	Connected experiences
ourcu		د Sharing across profiles >
😂 Groups	Tools and resources	→) Logging in with accounts >
Video	Our tools help you control and manage your privacy.	Account settings
	A Privacy Checkup	
न Marketplace	(Supervision	Password and security >
9 Find friends	Ø Default audience settings	Personal details
	Preferences	Your information and permissions
		4
L	4	• Facebook
÷	Tura factor	Add extra security to
Password and security	authentication	your account
Login & recovery Manage your passwords, login preferences and recovery methods.	Choose an account to set up two-factor authentication.	Two-factor authentication protects your account by requiring an additional code when you log in on a device we don't recognize. Learn more
Change password >	G Facebook	Choose your security method
Two-factor authentication		Authentication ann
		Huthenticution upp
Saved login (?) >		Recommended • We'll recommended an app to download if you don't have one. It will
Saved login Security checks Review security issues by running checks across apps. devices and emails sent.		Recommended • We'll recommended • We'll recommend an app to download if you don't have one. It will generate a code you'll enter when you log in. SMS or WhatsApp
Saved login Security checks Review security issues by running checks across apps, devices and emails sent. Where you're logged in		Recommended - We'll recommended - We'll recommended - We'll if you don't have one. It will generate a code you'll enter when you log in. SMS or WhatsApp We'll send a code to the mobile number you choose.
Saved login ♥ Security checks Review security issues by running checks across apps, devices and emails sent. Where you're logged in > Login alerts >		Recommended - We'll Recommended - We'll recommended - We'll generate a code you'll enter when you log in. SNS or WhatsApp We'll send a code to the mobile number you choose. Security keys Use physical security keys to
Saved login Security checks Review security issues by running checks across apps, devices and emails sent. Where you're logged in Login alerts Recent emails		Recommended - We'll Recommended - We'll recommended - We'll generate a code you'll enter when you log in. SNS or WhatsApp We'll send a code to the mobile number you choose. Security keys Use physical asecurity keys to protect your account from unauthorized access. You must have this key with you to log in
Saved login ()> Security checks Review security issues by running checks across apps, devices and emails sent. Where you're logged in Login alerts Recent emails Security Checkup >		Recommended - We'll recommended - We'll recommended - We'll generate a code you'll enter when you log in. SMS or WhatsApp We'll send a code to the mobile number you choose. Security keys Use physical security keys to protect your account from unauthorized access. You must have this key with you to log in from an unrecognized device.

Review Login Activity & Sign Out of Unrecognized Devices:

Regularly check where your account is logged in to ensure no unauthorized access.

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\diamondsuit) at the top.
- 3. Tap See more in Account Center > Password & Security > Where You're Logged In.
- 4. Select the account to check and review the list of active sessions.
- 5. If you see any unfamiliar locations or devices, select it and log out immediately



Menu \longrightarrow \otimes Q	< Settings & privacy Q	X Ø Meta	÷	÷
₩ ♥ ₽ <u>=</u> 7		Accounts Center	Password and security	Where you're logged in
Create new profile or Page	CO Meta Accounts Center Manage your connected experiences and account settings across Meta technologies.	Manage your connected experiences and account settings across Meta technologies like Facebook, Instagram and Meta Horizon. Learn more	Login & recovery Manage your passwords, login preferences and recovery methods.	See what devices are used to log in to your accounts. Set up alerts Accounts
login.		Profiles	Change password >	
🔇 Memories	Password and security Ad preferences	> Profiles	Two-factor authentication >	0 V >
	O Verification	Connected experiences	Saved login 🛛 😝 >	+ 8 more
Saved	See more in Accounts Center	Sharing across profiles >	Security checks	
😩 Groups	Tools and resources	→ Logging in with accounts >	Review security issues by running checks across apps, devices and emails sent.	
Video	Our tools help you control and manage your privacy.	Account settings	Where you're logged in	
📅 Marketplace	Supervision	Password and security	Login alerts >	
Find friends	Default audience settings	Personal details >	Recent emails (?) >	
	Preferences	Fa Your information and > permissions	Security Checkup (3 >	

Set up Login Alerts:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\bigcirc) at the top.
- 3. Tap See more in Account Center > Password & Security > Login Alerts.
- 4. Select the account to set up and choose preferred method of notification (email or in-app notifications)

Menu → @ Q @ C [®] 중 V [●] C [●] Ξ	C Settings & privacy Q	X 00 Meta	÷	÷		
7		Accounts Center	Password and security	Login alerts Manage how you'd like to be notified about unrecognized logins to your accounts.		
Create new profile or Page	00 Meta Accounts Center Manage your connected experiences and account settings across Meta technologies.	Manage your connected experiences and account settings across Meta technologies like Facebook, Instagram and Meta Horizon. Learn more	Login & recovery Manage your passwords, login preferences and recovery methods.			
login.			Change password >			
🕓 Memories	 Password and security Ad preferences 	Profiles >	Two-factor authentication >			
	⊘ Verification	Connected experiences	Saved login (?) >			
Saved	See more in Accounts Center	Sharing across profiles	Security checks			
😩 Groups	Tools and resources	→ → → → → → → → → → → → → → → → → → →	apps, devices and emails sent.			
💽 Video	Our tools help you control and manage your privacy.	Account settings	Where you're logged in >			
न Marketplace	Supervision	Password and security >	Login alerts < 🔿			
Find friends	Default audience settings	Personal details >	Recent emails () >			
	Preferences	Fa Your information and > permissions	Security Checkup (?) >			

Managing How People Find and Contact You:

1. Open Facebook and tap the **Menu Icon** (≡) in the top right.



- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Scroll down and choose **How People Find and Contact You** under *Audience and Visibility.*
- 4. Adjust settings for:
 - Who can find you using your phone number or email
 - Whether search engines outside Facebook can link to your profile
 - Who can see your friends list

Customize these options based on your privacy preferences.

Menu> 🕸 🔾	< Settings & privacy C	C Kow people find and contact			
a 🔮 🖩 \land 📮 	Audience and visibility Control who can see what you share on Facebook.	Your friends Who can send you friend requests? > Everyone			
Create new profile or Page Switch between profiles with one login.	 How people find and contact you Posts 	Who can see your friends list?			
C Memories	D Stories	Who can Facebook suggest your profile to based on your phone number or email address?			
Saved	 Followers and public content 	It someone has your phone number or email address, you can choose if you want to be suggested to them based on that information. Learn more			
😬 Groups	 Profile and tagging Blocking 	People with your email address			
🕑 Video	Active status	People with your phone number >			
<mark>न</mark> Marketplace	Payments Manage your payment info and activity.	Do you want search engines outside of Facebook to link to your profile?			
Find friends	S Payouts	When this setting is on, search engines may link to your profile in their results.			
	Your activity	When this setting is off, search engines will stop linking to your profile, but this may take			

Manage and Limit Posts:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Scroll down and choose Posts under Audience and Visibility.
- 4. Adjust settings for Who can see your future posts
 - Customize these options based on your privacy preferences.
- 5. Optional Select Limit who can see past posts to limit audience to Friends only





Manage Tags in Posts:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\diamondsuit) at the top.
- 3. Scroll down and choose Activity Log under Your Activity.
- 4. Tap Your Facebook Activity and then Manage Posts and Manage Tags
 - Customize these options based on your privacy preferences.



Manage Profile Visibility and Tags:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Scroll down and choose Profile and tagging under Audience and visibility.
- 4. Adjust settings for:

ODI AN

- Who can post on your profile
- Who can see what others post on your profile
- Who can see posts you're tagged in

Customize these options based on your privacy preferences.

Menu 🕸 🔾	C Settings & privacy Q	C Profile and tagging		
🙆 🔮 📾 🝼 🖆 💻	Audience and visibility	Viewing and sharing		
7	Control who can see what you share on Facebook.	Who can post on your profile?		
	Profile details			
Create new profile or Page	$\overset{\bigcirc \circ}{\frown}$ How people find and contact you	Volume of the set of t		
login.	🛱 Posts			
	Stories			
🔇 Memories	Reels			
Saved	Followers and public content			
	Profile and tagging			
😬 Groups	e Blocking €	Tagging and implied mentions Who can see posts you're tagged in on your profile?		
🕑 Video	Active status			
		Only me		
📅 Marketplace	Payments Manage your payment info and activity.	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?		
Find friends	(S) Payouts			
	Your activity	- Only me		

This document is published by the Open Digital Literacy and Access Network as an open source resource. For questions or modifications, please contact info@odlan.ca. This work is licensed under CC BY-NC 4.0.



Manage Public Content Your Followers See:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Scroll down and choose Followers and public content under Audience and visibility.
- 4. Adjust settings for **Who can see people, Pages and lists you follow**
 - Customize these options based on your privacy preferences.

Menu> 🕸 🔍	< Settings & privacy Q	K Followers and public content		< Choose audience
@ @	Audience and visibility Control who can see what you share on	Who can follow me Friends	> 1	Who can see the people, Pages and lists you follow?
· · · / · ·	Facebook. Profile details	Let anyone follow you Turn on professional mode to let		Remember, the people you follow can see that you're following them.
Create new profile or Page	$\overset{\bigcirc \circ}{\frown}$ How people find and contact you	people who are not your friends follow your public posts, reels and	(Anyone on or off Facebook
login.	Posts	stories.		Friends
	1 Stories	Try professional mode		Priends excent
🔇 Memories	Reels	Who can see your followers on your	-	Don't show to some friends
Saved	Followers and public content	timeline Only me	> .	Specific friends Only show to some friends
	Profile and tagging	Who can see the people, Pages and	. 1	🕒 Only me 📃 🔘
📇 Groups	Slocking	Only me	>	Only me
ዾ Video	Active status	Who can comment on your public posts? Friends		
न Marketplace	Payments Manage your payment info and activity.	Public post notifications Only me		
Find friends	S Payouts	Public profile info Friends		Save
	Your activity	Show most relevant comments		

Manage Apps and Websites Access to Your Facebook Account:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Scroll down and choose **Apps and websites** under *Your activity*.
- Review apps or websites with access and change or remove access based on preferences




Manage Activity Outside of Meta:

- 1. Open Facebook and tap the **Menu Icon** (≡) in the top right.
- 2. Select the **Settings Icon** (\mathfrak{Q}) at the top.
- 3. Tap See more in Account Center > Your Information & Permissions > Your Activity Off Meta Technologies.
- 4. Clear Previous Activity: Remove data linked to external sites and apps.
- 5. **Manage Future Activity:** Select **Disconnect Future Activity** to prevent tracking from external sources.

Menu \longrightarrow $ \otimes $ Q	< Settings & privacy Q	X Ø Meta	¢	÷
œ º œ º ⊄ = 7		Accounts Center	Your information and	Your activity off Meta
	Ø Meta Accounts Center	Manage your connected experiences and account settings across Meta	permissions	Your activity off Meta technologies includes
Create new profile or Page Switch between profiles with one	Manage your connected experiences and account settings across Meta technologies.	and Meta Horizon. Learn more	Access your information () >	share with us about your interactions with them such as visiting their apps or websites.
login.	 Personal details Password and security 	Profiles >	Download your information >	Learn more about activity off Meta technologies
C Memories	Ad preferences Verification	Connected experiences	Transfer a copy of your > information	What you can do
Saved	See more in Accounts Center		Search history >	You can control or disconnect the information businesses send to Meta.
😁 Groups	Tools and resources	 ∠→ Sharing across profiles > →) Logging in with accounts > 	View, download or transfer your information and activity on our apps.	Recent activity You have no available activity to show at this time
Video	Our tools help you control and manage your privacy.	Account settings	Your activity off Meta	Disconnect specific activity
异 Marketplace	Supervision	O Password and security >	Upload contacts >	Clear previous activity
Find friends	Default audience settings	Personal details	use to influence your experiences.	C Manage future activity >
	Preferences	Permissions		

 Clear previous activity The activity off Meta tachnologies includes from the usafresses and organizations send us about your interactions with them the usafresses and organizations send us about your interactions with them. Instagram Charn previous activity Instagram Concert future activity Well disconnect from alone the information the usafresses and organizations send us about your interactions with them. Concert future activity Well disconnect from alone the information the usafresses and organizations send us about your interactions with them. Concert future activity Well disconnect from alone the information the usafresses and organizations send us about your interactions with them. Concert future activity of information the usafresses and organizations send us about your interactions with them. Concert future activity or information the usafresses and organizations send us about your interactions with them. Concert future activity or information the usafresses and organizations send us about your interactions with them. Concert future activity or information the usafresses and organizations send us about your interactions with them. Concert future activity to information the usafresses and organizations send us about your interactions with them. Concert future activity or information the usafresses and organizations send us about your interactions with them. Concert future activity activity or information the usafresses and organizations send us about activity or information the usafresses and organizations send us about your information the usafresses. Well disconnect from the usafresses and organizations send usafresses. Well send concertse well well well well well well well we	÷	~	<i></i>	What you should know
Verr activity Verr activity of Meta technologies includes Instagram Verr activity of Meta technologies Instagram Verr activity of Meta technologies Instagram Control of disconnect the information that businesses and organizations such them. Instagram Control of disconnect the information that businesses and organizations such them. Instagram Control of disconnect the information that businesses and organizations such them. Instagram Control of disconnect the information that businesses and organizations such them. Instagram Control of disconnect the information that businesses and organizations such them. Instagram Control of disconnect the information that businesses and organizations such them. Instagram Control of disconnect the information that businesses and organizations such uses of the information that businesses and organizations such uses of the information that businesses and organizations such uses of the information that businesses and organizations such use use of the information that businesses and organizations such uses of the information that businesses and organizations such use use of the information that businesses and organizations such use use of the information that businesses and organizations such use use of the information that businesses and organizations such use use of the information that businesses and organizations such use use use of the information that businesses and organizations such use	Clear previous activity Your activity history will be disconnected from	Your activity off Meta technologies	Manage future activity Used for 1 account ∨	When you disconnect your future activity that businesses send us, your choices will annling to all of your acroants you've links
 Instagram Instagra	Clear previous activity	Your activity off Meta technologies includes information that businesses and organizations share with us about your iteractions with them such as visiting their apps or websites.	Connect future activity We'll connect information that businesses and organizations send us about your interactions with them. This is your current experience.	We'll disconnect future activity from your account. It may take 48 hours until it's fully
You have no available activity to > Show at this time. > Ø Disconnect specific activity > Image future activity > Image future activity > Continue Continue	@ Instagrom	Mean more about activity off Meta technologies Mota you can do You can control or disconnect the information businesses send to Meta. O Recent activity	Disconnect future activity We'll disconnect information that businesses and organizations send us about you'n theractions with them. Hypu decide to disconnect your future activity, we'll also char your previous activity.	 disconnected from your account. If you're logged into any apps and website with Facebook, disconnecting future activ may log you out. If you're connected your Instagram profile to other apps and websites, disconnecting your future activity may stop your Instagram profile from being connected to those businesses.
 Clear previous activity 		You have no available activity to show at this time.		OD We'll still receive activity from apps and websites. It may be used for measuremer purposes and to make improvements to our ads systems, but it will be disconnect from your account.
Continue Disconnect future activity		Clear previous activity >		You'll still see the same number of ads, bu the ads you see may be less personalized you. View your Ad Preferences.
			Continue	Disconnect future activity

TikTok Security & Privacy Settings

Updating Your Password to a Strong and Unique One:

- 1. From Profile, tap the **Menu Icon** (≡) in the top right.
- 2. Select Settings and Privacy > Account > Password
- 3. Verify your email and follow on-screen instructions to enter a new, strong password and confirm the change

Fotowing F	∰ θρ ≡	φ ₀ =	4	← Account
Followers Les Followers Les Account Password > Edit profile Share profile Privacy Security & permissions > Perfication > III - 1 <t< th=""><th>1</th><th></th><th>Settings and privacy</th><th>Account information ></th></t<>	1		Settings and privacy	Account information >
Following Fo			Account	Password 🡉 >
Following Fo			🛔 Account 🧹 >	Passkey >
Edit profile Share profile Image:	Following Followers Likes		Privacy >	Set up a passkey to log in to TikTok with Android Face or Touch Unlock. TikTok can't access this biometric data.
III- A III- A III- A III- A III- A III- A Content & Display Download your data III- A III- A Content & Display Download your data III- A III- A III- A IIII- A III- A III- A III- A <th>Edit profile Share profile</th> <th></th> <th>Security & permissions</th> <th>Verification</th>	Edit profile Share profile		Security & permissions	Verification
Image: Content & Display Download your data Dow			✤ Share profile >	Switch to Business Account
Image: Provide and prov	;;;+ A t }		Content & Display	Download your data >
Image: Weight of the strain			Notifications >	Get a copy of your data from all the TikTok apps you use.
Image: Provide and privacy Image: Provide and privacy <th></th> <th></th> <th>ŭ LIVE →</th> <th>Deactivate or delete account ></th>			ŭ LIVE →	Deactivate or delete account >
Image: Content preferences Image: Content preferences Image: Content preferences		⊱ TikTok Studio	Activity center >	
Image: Control of the second secon		🗂 Balance	Content preferences	
Concerne Prince The Concernence of Settings and privacy Concernence of Ads		8% My QR code	Audience controls	
	Home Friends Inbox Profile	O Settings and privacy	ngl Ads >	

Setting Up Two-Factor Authentication (2FA):



- 1. From Profile, tap the **Menu Icon** (\equiv) in the top right.
- 2. Select Settings and Privacy > Security & Permissions > 2-Step Verification
- 3. Select at least 2 verification methods (e.g. Phone, Email, Authenticator or Password) and turn on

tin 80 ≡		\leftarrow	← Security & permissions	\leftarrow
1		Settings and privacy	Security	2-step verification is off
		Account	Security alerts >	Turning this on will require an additional verification code when you log in from an untrusted device. Learn more
		🚢 Account >	Manage devices >	Select at least 2 methods
Following Followers Likes		🔒 Privacy >	2-step verification Off >	Phone You'll receive a verification code via SMS.
Edit profile Share profile 🔑		Security & permissions	Save login info	S Email
		✤ Share profile >	Log in on this device without needing to enter your info, or on a new device when you restore your backup.	You'll receive a verification code at
tì 🗟 ©		Content & Display	Permissions	Authenticator
		Notifications >	Apps and services permissions \rightarrow	Install an app to generate your verification code.
		🛍 LIVE >	Browser settings >	🔒 Password 🛛 🧹
	P _★ TikTok Studio	Activity center		
	🗇 Balance	Content preferences		
	8% My QR code	Let Audience controls		
습 옷 (+) 문 <mark>양 옷</mark> Home Friends Inbox Profile	O Settings and privacy	Madas >		Turn on

Review Security Alerts Detected:

- 1. From Profile, tap the **Menu Icon** (≡) in the top right.
- 2. Select Settings and Privacy > Security & Permissions > Security Alerts
- 3. Review any security alerts of unusual activity in the last 7 days

^(†) 89 ≡		\leftarrow	← Security & permissions	÷
1		Settings and privacy	Security	
		Account	Security alerts	
•		Account	Manage devices >	
Following Followers Likes		A Privacy	2-step verification Off >	~
Edit profile Share profile		Security & permissions	Save login info	
		Share profile	Log in on this device without needing to enter your info, or on a new device when you restore your backup.	No unusual account activity detected in the last 7 days.
##• 🔂 🕼 🕼		Content & Display	Permissions	
		Notifications >	Apps and services permissions $\qquad \qquad >$	
		Ď LIVE →	Browser settings	
	Arr TikTok Studio	Activity center >		
	🗇 Balance	Content preferences		
	89 My QR code	Let Audience controls		Done
Home Friends + F	O Settings and privacy	ngl Ads		Still have questions? Contact us

This document is published by the Open Digital Literacy and Access Network as an open source resource. For questions or modifications, please contact info@odlan.ca. This work is licensed under CC BY-NC 4.0.



Review Devices Logged into your Account:

- 1. From Profile, tap the **Menu Icon** (≡) in the top right.
- 2. Select Settings and Privacy > Security & Permissions > Manage Devices
- 3. View list of devices logged into your account and delete any unfamiliar devices

👘 8g 🚍		\leftarrow	← Security & permissions	÷
1		Settings and privacy	Security	Manage devices
		Account	Security alerts	
l l		🛔 Account >	Manage devices 🧼 💦	Current device
Following Followers Likes		🚔 Privacy >	2-step verification Off >	TikTok App Unknown login method
Edit profile Share profile 🔎	Edit profile Share profile	Security & permissions	Save login info	
		Share profile	Log in on this device without needing to enter your info, or on a new device when you restore your backup.	Other devices you've logged in on ③
III• A 🗘 🗔 ଭ		Content & Display	Permissions	TikTok App
		Notifications >	Apps and services permissions >	
		🛍 LIVE >	Browser settings >	
	$ ho_{m{\star}}$ TikTok Studio	S Activity center >		
	🗇 Balance	Content preferences		
	器 My QR code	Le Audience controls		
습 옷 + Filends Profile	© Settings and privacy	nd Ads		

Disable Downloads from Others:

- 1. From Profile, tap the **Menu Icon** (\equiv) in the top right.
- 2. Select **Settings and Privacy > Privacy > Scroll down to Downloads**
- 3. Toggle off so other people can't download your videos

👘 99 🚍		\leftarrow	+ Privacy	← Downloads
1		Settings and privacy	Manage the location information TikTok uses to personalize your experience	Since your account is private, other people can't download your videos.
		Account	Interactions	Video downloads
		Account >	Comments	
Elliptica Elliptica de la		A Privacy 🧹 🔿		
Following Followers Likes		Security & permissions >	@ Mentions >	
Edit prome Share prome 7		Share profile	Direct messages Everyone >	
			Reuse of content >	
₩ - & t) & ©		Content & Display	± Downloads	
		Notifications >	* Following list Followers >	
		ŭ LIVE →	Liked videos Followers >	
	A TikTok Studio	Activity center	■ Favorite sounds Off >	
	🔂 Balance	Content preferences	► Post views On >	
	8% My QR code	Let Audience controls	Profile views Off >	
Home Friends - Friends	O Settings and privacy	Mil Ads >	S Blocked accounts	

This document is published by the Open Digital Literacy and Access Network as an open source resource. For questions or modifications, please contact info@odlan.ca. This work is licensed under CC BY-NC 4.0.



Disconnect Contacts and Facebook Friends:

- 1. From Profile, tap the **Menu Icon** (≡) in the top right.
- 2. Select Settings and Privacy > Privacy > Sync contacts and Facebook Friends
- 3. Toggle Sync Contacts and Sync Facebook Friends off
- 4. Remove previously synced contacts and Facebook friends



Adjust Additional Privacy Settings for Account Interactions:

- 1. From Profile, tap the **Menu Icon** (≡) in the top right.
- 2. Select **Settings and Privacy** > **Privacy** > Scroll down to the *Interactions* section
- 3. Adjust settings based on preferences for Comments, Mentions, Direct Messages, Following List, Views etc.



a a a		L	/ Drivery	
1		Settings and privacy	Manage the location information personalize your experience	
		Account		
ļ		🛔 Account >	Interactions	
		Privacy	Comments	
Following Followers Likes		Convitu 8 norminaire	@ Mentions	
Edit profile Share profile		Seconty & permissions	Direct messages	
		Share profile	Reuse of content	
#F 🔂 🔂 🕬		Content & Display	🛨 Downloads	
		Notifications >	🏝 Following list	
		LIVE >	Liked videos	
	P̂★ TikTok Studio	Activity center >	Favorite sounds	
	🗇 Balance	Content preferences	Post views	
	器 My QR code	Le Audience controls	Profile views	
습 우 (+) 문 <mark>양 오</mark> Home Friends Inbox Profile	© Settings and privacy	nd Ads →	S Blocked accounts	

Disconnect Third Party Apps from Connecting to your Account:

- 1. From Profile, tap the **Menu Icon** (≡) in the top right.
- Select Settings and Privacy > Security & Permissions > Apps and Services Permissions
- 3. Disconnect any authorized apps from connecting to your TikTok account

[®] 9 ≡		\leftarrow	← Security & permissions	Apps and services permissions
1		Settings and privacy	Security	
		Account	Security alerts	
'		Account >	Manage devices >	
Following Followers Likes		A Privacy	2-step verification Off >	
Edit profile Share profile 🔎	Edit profile Share profile	Security & permissions	Save login info	\smile
		Share profile	Log in on this device without needing to enter your info, or on a new device when you restore your backup.	No apps authorized yet
III• A 🕻 🖟 👒		Content & Display	Permissions	with your netox account will appear here.
		Notifications >	Apps and services permissions	
		ŭ LIVE →	Browser settings	
	P★ TikTok Studio	Activity center >		
	🗇 Balance	Content preferences		
	89 My QR code	Let Audience controls		
Home Friends Inbox Profile	Q Settings and privacy	nd Ads		

For more information on securing your social media profiles check out

• How to Change your Meta Settings https://www.johnoliverwantsyourraterotica.com/



- Social Media Security & Privacy Checklist https://docs.google.com/document/d/1ud1lLFkIG0BeLX9jlzJMxCPm8-cSeqPjU60nkhUPYA8/edit?usp=sharing
- The checklist is from a New York Times article: Kozinski, K. & Kapur, N. (2020, February 27). *How to Dox Yourself on the Internet*. New York Times. <u>https://open.nytimes.com/how-to-dox-yourself-on-the-internetd2892b4c5954</u>

4.4.4. Doxxing and Public Information Protection

- **Doxxing:** Doxxing is the act of publicly exposing an individual's private or sensitive information without their consent, often for harassment or intimidation. This can include home addresses, phone numbers, workplace details, and personal communications. To mitigate the risks of doxxing, individuals should take proactive measures to secure their online presence.
- **Proactive Measures**: Strengthening privacy settings on social media and online accounts is crucial. Limiting the visibility of personal details such as contact information, location data, and workplace affiliations can reduce exposure. Secure communication methods, such as encrypted messaging and multi-factor authentication, further protect personal data. Additionally, using pseudonyms or aliases for non-professional online interactions can help prevent personal details from being linked back to an individual.
- Limit Personal Information Exposure: Avoid sharing personal details like phone numbers, addresses, or employer names publicly. Be mindful of metadata embedded in images and documents, as this can unintentionally reveal sensitive information. For more information, check out <u>this article here for examples of what can be collected</u>.
 Opting out of data broker websites that collect and sell personal information can further reduce the risk of exposure.
- **Monitor & Respond to Threats:** Set up Google Alerts for your name and other sensitive identifiers can help you stay informed about any public mentions of your information. Regularly search for your information online and request removals from data aggregator sites.
- Check out these resources for more information on how to protect yourself against doxxing
 - <u>https://equalitylabs.medium.com/anti-doxing-guide-for-activists-facing-attacks-</u> from-the-alt-right-ec6c290f543c
 - https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954
 - https://righttobe.org/guides/how-to-strengthen-your-digital-security/
 - <u>https://pen.org/digital-safety-snacks/</u>

4.5. Personal Device Security

• **VPN Use:** Employees must enable recommended VPN (virtual private network) on all personal and professional devices used for accessing organizational resources, including laptops, smartphones, and tablets.



- Company must decide which VPN is preferred, and IT Team is responsible for set up and troubleshooting if needed. Also, if there are device management softwares used, if the VPN works properly within that controlled environment.
- A VPN (Virtual Private Network) creates a secure connection between your device and the internet. This encrypts data being sent and received for your privacy. VPNs hide your IP address, making it more difficult for cybercriminals to track your online activity or intercept sensitive information. VPNs are essential for protecting networks from cyber threats, particularly when accessing the organization's resources remotely, as they help safeguard confidential data and prevent unauthorized access.
 - Many VPNs are free to use, however they usually will share your data so a paid VPN is preferred. For a comprehensive analysis of available VPNs, please check this resource:
 - <u>https://docs.google.com/spreadsheets/d/1ijfqfLrJWLUVBfJZ_YalVpstWsjw-JGzkvMd6u2jqEk/edit?gid=231869418#gid=231869418</u>

r/VPN [paperplans5]. (2021, March 17). *VPN Comparison Table* [Online forum post]. Reddit. <u>https://www.reddit.com/r/VPN/comments/m736zt/vpn_comparison_table/</u>

- List of Recommended VPNs:
 - Proton <u>https://protonvpn.com/</u>
 - Mozilla Firefox VPN <u>https://www.mozilla.org/en-US/products/vpn/</u>
 - CyberGhost VPN <u>https://www.cyberghostvpn.com/</u>

For more details, visit: Government of Canada's Get Cyber Safe VPN resources https://www.getcybersafe.gc.ca/en/secure-your-connections/vpns

- **Regular Updates:** Employees should regularly update the operating systems and software on their personal devices to protect against vulnerabilities when prompted, or upon request by the IT Team. It is recommended that full updates be made every (preferred frequency).
- Security Software: Employees must install and maintain security software, such as antivirus and anti-malware programs, on personal devices used for work purposes. Below are some recommended antivirus softwares.
 - Norton <u>https://ca.norton.com/?IsModal=1#</u>
 - Norton provides real-time threat protection against malware, ransomware, phishing, and other cyber threats. It includes additional security features such as a password manager, firewall protection, and identity theft monitoring. Norton offers various paid plans tailored to different security needs.
 - McAfee https://www.mcafee.com/en-us/antivirus.html
 - McAfee delivers 24/7 virus protection with an advanced firewall to prevent unauthorized access. It includes privacy-focused features such as



Personal Data Cleanup, a Social Privacy Manager, a secure VPN, and identity theft monitoring.

- Bitdefender https://www.bitdefender.com/en-us/consumer/free-antivirus
 - Bitdefender offers antivirus protection for both Windows and macOS, with the option to choose between free and paid versions. It provides daily virus scans, real-time protection, and safeguards against a wide range of cyber threats.

Note: Company must decide which software is preferred, and the IT Team is responsible for setting up and troubleshooting if needed.

- Ad Blocking Browser Extensions: Employees must enable recommended Ad blocking browser extensions on all personal and professional devices used for accessing organizational resources, including laptops, smartphones, and tablets.
- Ad blockers help remove or hide advertisements from web pages, reducing exposure to malicious ads that may lead to harmful sites or contain malware. They also enhance privacy by preventing web trackers from collecting browsing data. Many ad blockers are available as browser extensions and can be installed on Chrome, Firefox, Edge, and other browsers.
- Recommended ad blockers based on the browser you use:
 - Google Chrome
 - ABP Adblock Plus - <u>https://chromewebstore.google.com/detail/adblock-plus-free-ad-</u> bloc/cfhdojbkjhnklbpkdaibdccddilifddb
 - AdBlock <u>https://chromewebstore.google.com/detail/adblock-</u> %E2%80%94-block-adsacros/gighmmpiobklfepjocnamgkkbiglidom
 - Mozilla Firefox
 - uBlock Origin <u>https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/</u>
 - AdBlocker Ultimate <u>https://addons.mozilla.org/en-US/firefox/addon/adblocker-ultimate/</u>
 - Microsoft Edge
 - AdGuard AdBlocker -<u>https://microsoftedge.microsoft.com/addons/detail/adguard-</u> adblocker/pdffkfellgipmhklpdmokmckkkfcopbh

4.6. Incident Response and Reporting

4.6.1. Reporting Security Incidents

• **Immediate Reporting:** Employees must report any suspected or confirmed compromise of their digital identity, such as unauthorized access to accounts or identity theft, to the IT department immediately.



• **Documentation:** When reporting an incident, employees should provide as much detail as possible, including the type of incident, affected accounts, and any suspicious activities observed.

4.6.2. Organizational Response

- Incident Investigation: The IT department will investigate reported incidents to determine the extent of the compromise and take appropriate actions to mitigate the impact.
- Account Recovery: The organization will assist affected employees in recovering compromised accounts and securing their digital identities. This may include password resets, account monitoring, and coordination with external services or law enforcement if necessary.

4.7. Training and Awareness

4.7.1. Employee Training

- **Initial Training:** All employees must complete training on protecting their digital identities upon joining the organization or when this policy is implemented.
 - For more details, please refer to your company onboarding handbook or reach out to the HR team for any questions or clarifications.
- **Ongoing Training:** The organization will provide ongoing training and resources to help employees stay informed about best practices in digital identity protection and emerging threats. Below are some training resources on cyber security awareness and online safety.
 - LinkedIn Learning has several cybersecurity courses and learning pathways available.
 - https://www.linkedin.com/learning/paths/build-your-cybersecurityawareness-skills
 - KnowBe4 provides a security awareness training program with real-world phishing simulations, learning management system and dashboard to track employee progress.
 - https://www.knowbe4.com/products/security-awareness-training
 - The InfoSec Institute offers employee cybersecurity training videos on topics such as phishing, social engineering, public wifi and physical security
 - <u>https://www.infosecinstitute.com/iq/work-bytes/</u>
 - Amazon has a cybersecurity awareness training that covers topics like secure communication, data classification, phishing, physical security, social engineering, data privacy, third-party/application security, laptop standard, protect data, and acceptable use.
 - https://learnsecurity.amazon.com/en/index.html

Check NIST's IT Lab for a list of Free and Low Cost Online Cybersecurity Learning Content: <u>https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content</u>



4.7.2. Awareness Campaigns

- **Regular Reminders:** The organization will conduct regular awareness campaigns to remind employees of the importance of protecting their digital identities and following security best practices.
- Information Sharing: The IT department will share relevant information about new threats, phishing attempts, or breaches that could impact employees' digital identities.

5. Incident Response

Crisis Response Plan for Threats on Organizational Social Media Accounts

5.1. Purpose

The purpose of this Crisis Response Plan is to provide a structured approach for handling threats to the organization's social media accounts. This plan aims to mitigate risks, protect the organization's reputation, and ensure a coordinated response to any threat that impacts social media channels.

5.2. Scope

This plan applies to all social media accounts managed by the organization, including corporate, departmental, and individual accounts related to the organization's brand and operations. It covers all types of threats, including security breaches, misinformation, harassment, and targeted attacks.

5.3. Crisis Response Team (CRT)

5.3.1. Team Composition

- **Crisis Manager:** Responsible for overseeing the response and making strategic decisions.
- **Social Media Manager:** Handles the immediate response on social media platforms and content moderation.
- IT Security Specialist: Manages technical aspects, including security breaches and account recovery.
- **Public Relations Officer:** Coordinates external communication and manages the organization's public image.
- Legal Advisor: Provides guidance on legal implications and regulatory compliance.



• **HR Representative:** Supports affected employees and manages internal communication.

5.3.2. Contact Information

- Crisis Manager: [Name, Contact Information]
- Social Media Manager: [Name, Contact Information]
- IT Security Specialist: [Name, Contact Information]
- Public Relations Officer: [Name, Contact Information]
- Legal Advisor: [Name, Contact Information]
- HR Representative: [Name, Contact Information]

5.4. Incident Detection and Assessment

5.4.1. Detection

- **Monitoring Tools:** Use social media monitoring tools to detect unusual activity or threats.
- **Employee Reporting:** Encourage employees to report any suspected threats or unusual activity on social media.

5.4.2. Assessment

- **Initial Evaluation:** Assess the nature and scope of the threat, including the type of threat (e.g., security breach, misinformation, harassment) and its potential impact.
- **Severity Rating:** Categorize the threat based on its severity (e.g., low, medium, high) to prioritize response actions.

5.5. Immediate Response Actions

5.5.1. Containment

- **Isolate Threat:** Take immediate steps to contain the threat, such as disabling compromised accounts, removing harmful content, or restricting access.
- **Secure Accounts:** Implement additional security measures, such as changing passwords, enabling multi-factor authentication, and reviewing account permissions.

5.5.2. Communication

- **Internal Notification:** Notify the Crisis Response Team and relevant internal stakeholders about the threat and initial response actions.
- External Communication: Prepare a holding statement to acknowledge awareness of the issue and that a response is being developed. Avoid detailed disclosures or speculations at this stage.

5.6. Detailed Response



5.6.1. Public Communication

- **Prepare Response Statements:** Develop clear, concise, and accurate statements for public release. Address the issue transparently, provide factual information, and outline steps being taken to resolve the situation.
- **Coordinate Messaging:** Ensure consistent messaging across all communication channels and avoid contradicting statements from different departments or team members.

5.6.2. Technical Response

- **Investigate Incident:** Conduct a thorough investigation to determine the cause and impact of the threat. Document findings and response actions.
- **Mitigate Damage:** Implement technical solutions to address and resolve the issue, such as patching vulnerabilities, removing malware, or recovering compromised data.

5.7. Recovery and Resolution

5.7.1. Restore Normal Operations

- Account Restoration: Restore affected social media accounts to normal operation, ensuring that all security measures are in place and verified.
- **Content Review:** Review and clean up any compromised or harmful content from social media channels.

5.7.2. Post-Incident Actions

- **Impact Assessment:** Evaluate the impact of the threat on the organization, including damage to reputation, operational disruption, and any legal or regulatory implications.
- **Communication Follow-Up:** Provide updates to stakeholders and the public as necessary, and continue to address any remaining concerns or questions.

5.8. Post-Crisis Review

5.8.1. Incident Analysis

- **Debriefing:** Conduct a debriefing session with the Crisis Response Team to review the response actions, identify what worked well, and discuss areas for improvement.
- **Documentation:** Create a comprehensive report detailing the incident, response actions, and outcomes. Include lessons learned and recommendations for future preparedness.

5.8.2. Policy and Procedure Updates

• **Review and Update:** Review and update social media security policies, crisis response procedures, and training materials based on lessons learned from the incident.



• **Training and Drills:** Conduct regular training and simulation exercises for the Crisis Response Team and relevant employees to ensure preparedness for future incidents.

5.9. Ongoing Monitoring and Improvement

5.9.1. Monitor for Recurrence

- **Continuous Monitoring:** Maintain ongoing monitoring of social media channels to detect any signs of recurring threats or related issues.
- **Proactive Measures:** Implement proactive measures to strengthen social media security and prevent similar incidents in the future.

5.9.2. Feedback and Improvement

- **Gather Feedback:** Collect feedback from the Crisis Response Team, employees, and stakeholders on the effectiveness of the response plan and areas for improvement.
- **Plan Updates:** Regularly review and update the crisis response plan to incorporate new threats, changes in social media platforms, and emerging best practices.

6. Incident Response Strategy for Email Accounts Receiving Hate Mail

6.1. Purpose

This strategy outlines the steps to be taken when an organization's email accounts are being targeted with hate mail. The goal is to protect employees, mitigate disruption, and prevent further escalation.

6.2. Scope

This strategy applies to all email accounts associated with the organization, including those of employees, executives, and shared departmental addresses. It covers incidents involving the receipt of hate mail, including threats, harassment, and abusive language.

6.3. Incident Detection

6.3.1. Indicators of Hate Mail

- Receipt of multiple emails containing abusive, threatening, or hateful language.
- Emails targeting specific individuals or groups within the organization based on characteristics such as race, gender, religion, or sexual orientation.



- High volume of unsolicited emails from unknown or suspicious senders.
- Emails containing malicious attachments, links, or images.

6.4. Immediate Response Steps

6.4.1. Employee Actions

- **Do Not Respond:** Employees should not respond to or engage with the sender of hate mail.
- **Report Immediately:** Do not forward hate mail. Send a screenshot to the IT department or designated security team with the subject line "Hate Mail Incident." If the email contains threats, escalate immediately to senior management and security.
- **Preserve Evidence:** Retain a copy of the email(s) without deleting or altering any content. This evidence may be necessary for investigation or legal action. Create a folder in Gmail to collect evidence.
- **Responsibility Assignment**: Define who collects evidence and organizes the folder system. Ensure marginalized team members (e.g., trans, nonbinary, BIPOC employees) are not required to manage these tasks.

6.4.2. IT Department/Security Team Actions

- Assess the Threat:
 - **Content Analysis:** Review the content of the hate mail to assess the severity of the threat, including any potential harm to individuals or the organization.
 - **Source Identification:** Trace the source of the hate mail, including IP addresses, domains, and other identifying information, to determine whether it is part of a larger attack or a targeted harassment campaign.
- Implement Defensive Measures:
 - **Block Senders:** Block the sender's email address and any associated IP addresses or domains to prevent further emails from being received.
 - **Review Security Logs:** Analyze email system logs to identify patterns or unusual activity related to the hate mail and monitor for further incidents.
 - **Email Filters:** Update spam and threat filters to automatically detect and quarantine similar emails in the future.
 - i. Go to 'manage labels' on side bar. Select 'filters and blocked addresses.
 - ii. Select keyword for filter.
 - iii. Select 'Create filter' button, and select option for action.
 - iv. Not sure what to filter? Try

https://web.archive.org/web/20240418094602/https://www.freewebheader s.com/full-list-of-bad-words-banned-by-google/

ODLAN ED = 附 Gmail Q Search mail 뀶 2 Settings 🖉 Compose General Labels Inbox Accounts Filters and Block Forwarding and POP/IMAP Add-ons Chat and Meet Advanced Offline Themes 🖂 Inbox 33 System labels Show in label list Chat ☆ Starred Inbox œ Snoozed Starred show hide ▷ Sent show hide Snoozed Drafts show hide Less Important ∑ Important Sent show hide Bo Scheduled Scheduled show hide show if unread 🖾 🛛 All Mail Drafts show hide show if unread ① Spam All Mail show hide 🗊 Trash → □ Categories Spam show hide show if unread Manage labels Formatter of the second seco Trash show hide Show in label list Show in message list Categories show hide Labels Categories Social show hide show hide Updates show hide show hide Forums show hide show hide show hide Promotions show hide Create new label Show in label list Show in message list Actions Note: Removing a label will not remove the messages with that label.

≡	M	Gmail		Q Search mail								
Mail	1	Compose		From		 			ons	Chat and Meet	Advanced	0
Chat	⊠ ☆ © ₽	Inbox Starred Snoozed Sent Drafts	33 2	Subject Has the words Doesn't have Size	greater than	•	МВ	×				
		Important Scheduled All Mail Spam Trash		Has attachr	nent	 	Create filter Se	arch				
	。 令 十 Lab	Manage labels Create new label	+									



6.5. Containment and Mitigation

6.5.1. Contain the Threat

- **Isolate the Incident:** Isolate affected email accounts to prevent the spread of harmful content within the organization. This may include temporarily disabling email accounts or redirecting emails to a secure inbox for review.
- **Communicate Internally:** Notify relevant stakeholders, including the executive team, HR, and legal counsel, about the incident and the steps being taken to mitigate the threat.

6.5.2. Mitigate Impact on Employees

- Employee Support:
 - **Counseling Services:** Offer counseling or emotional support services to employees who have been targeted by hate mail.
 - **Training and Awareness:** Provide guidance on how to handle hate mail and avoid engagement with threatening or abusive senders.
- Legal Action: In cases involving severe harassment or credible threats, consult with legal counsel to explore options for pursuing legal action, such as filing a complaint with law enforcement or obtaining a restraining order.
 - The organization must establish clear circumstances on when legal authorities should be notified (e.g. bomb threats)



6.6. Recovery and Communication

6.6.1. System Recovery

- **Resume Normal Operations:** Once the threat is contained, restore normal email operations and ensure that security measures are in place to prevent future incidents.
- **Monitor for Recurrence:** Continue to monitor email traffic for any signs of recurring hate mail or related threats.

6.6.2. Internal Communication

- **Inform Employees:** Provide a brief to all affected employees on the incident, the steps taken to address it, and any additional precautions they should follow.
- **Policy Reinforcement:** Remind employees of the organization's policies on email use, security, and reporting suspicious or harmful emails.

6.6.3. External Communication

- **Media and Public Relations:** If the hate mail incident attracts public attention, coordinate with the public relations team to prepare a statement that addresses the situation while protecting the privacy of affected employees.
- **Clarify Notification Scope**: The organization must determine the level of public disclosure required, balancing transparency with employee protection.
- **Stakeholder Communication:** If necessary, communicate with key external stakeholders, such as clients or partners, to reassure them of the organization's commitment to maintaining a safe and secure environment.

7. Email Phishing Incident Response Strategy

7.1. Purpose

This strategy outlines the steps to be taken when an email phishing attempt is detected or suspected within the organization. The goal is to minimize the impact, prevent data breaches, and enhance the organization's overall cybersecurity posture.

7.2. Scope

This strategy applies to all employees, contractors, and third-party vendors who have access to the organization's email systems. It covers all forms of phishing, including spear phishing, whaling, and generic phishing attacks.



7.3. Incident Detection

7.3.1. Indicators of Phishing

- Unexpected emails from unknown or suspicious senders, especially those requesting sensitive information.
- Emails containing suspicious links or attachments.
- Urgent requests for personal, financial, or login information.
- Emails with poor grammar or unusual formatting.
- Unsolicited requests for login credentials, passwords, or account details.

7.4. Immediate Response Steps

7.4.1. Employee Actions

- **Do Not Engage:** Do not click on any links, open any attachments, or reply to the suspicious email.
- **Report Immediately:** Do not forward the phishing email. Send screenshots to the IT department or designated security team with the subject line "Suspected Phishing."
- **Isolate the Threat:** If a phishing link or attachment has been clicked, disconnect the device from the network immediately and inform IT.

7.4.2. IT Department Actions

- **Analyze the Email:** Investigate the reported email to determine if it is indeed a phishing attempt. Use tools to analyze links, attachments, and sender information.
- **Block and Quarantine:** Block the sender and quarantine the email across the organization's email systems to prevent further exposure.
- Scan Affected Systems: If the phishing email was interacted with, conduct a full malware and virus scan on the affected device(s).
- **Change Credentials:** If login credentials were compromised, immediately instruct the employee to change their passwords. Consider enforcing a system-wide password reset if necessary.

7.5. Containment and Eradication

7.5.1. Contain the Threat

- **Network Isolation:** If a device is compromised, isolate it from the network to prevent the spread of any potential malware or unauthorized access.
- **Data Access Review:** Review access logs to identify any unauthorized access to sensitive data or systems.

7.5.2. Eradicate the Threat



- **Remove Malware:** Remove any detected malware or unauthorized software from the compromised systems.
- **Patch Vulnerabilities:** Identify and patch any vulnerabilities that may have been exploited by the phishing attack.

7.6. Recovery and Communication

7.6.1. System Recovery

- **Restore Systems:** Restore any affected systems to their pre-attack state using clean backups.
- Monitor Systems: Monitor the restored systems for any signs of residual threat activity.

7.6.2. Internal Communication

- **Notify Stakeholders:** Inform relevant internal stakeholders about the phishing incident, including what was targeted, the impact, and the response actions taken.
- **Debrief Affected Employees:** Provide a debrief to employees who were targeted or affected by the phishing attack, including any necessary actions they should take.

7.6.3. External Communication

- **Notify External Parties:** If necessary, notify external parties such as customers, partners, or regulatory bodies about the incident, especially if sensitive data was compromised.
- **Public Relations:** Prepare a public statement if the incident is likely to become public knowledge, ensuring it is aligned with the organization's communication policies.

8. Social Media Account Incident Response Strategy

8.1. Purpose

The purpose of this strategy is to provide a clear and structured response plan for when an organization's social media account is compromised, attacked, or misused. This plan aims to minimize damage, restore security, and protect the organization's reputation.

8.2. Scope

This strategy applies to all social media accounts owned or operated by the organization, including those managed by employees, contractors, and third-party vendors. It covers incidents



such as account hacking, unauthorized access, impersonation, and the dissemination of harmful or misleading information.

8.3. Incident Detection

8.3.1. Indicators of Compromise

- Unauthorized posts, messages, or comments appearing on the account.
- Unexpected changes to account settings, profile information, or passwords.
- Sudden spikes in follower count or unusual engagement patterns.
- Notifications of login attempts from unfamiliar locations or devices.
- Reports from followers or employees about suspicious activity on the account.

8.4. Immediate Response Steps

8.4.1. Employee Actions (For those not responsible for platforms)

- **Report Immediately:** If you suspect the account has been compromised, report the incident to the IT department or the designated social media manager immediately.
- **Do Not Interact:** Avoid interacting with or attempting to delete suspicious content until the IT department has been notified.
- **Collect Information:** Document any suspicious activities, including screenshots, timestamps, and any relevant messages or notifications.

8.4.2. IT Department/Social Media Manager Actions

- Secure the Account:
 - **Change Passwords:** Immediately change the account password and enable multi-factor authentication (MFA) if not already enabled.
 - **Revoke Access:** Review and revoke access for any unfamiliar devices, applications, or users connected to the account.
 - **Review Admin Access:** Check and update the list of account administrators, ensuring that only authorized personnel have access.
- Communicate Internally:
 - Inform relevant stakeholders, including the communications team and executive leadership, about the incident and the steps being taken to secure the account.
 - Coordinate with the public relations team to prepare for external communication if needed.
- Account Recovery:
 - LinkedIn: <u>https://www.linkedin.com/help/linkedin/answer/a1342692</u>
 - Facebook account recovery instructions: <u>https://www.facebook.com/help/203305893040179</u>
 - Instagram account recovery instructions: <u>https://help.instagram.com/149494825257596</u>



- YouTube Channel account recovery instructions: <u>https://support.google.com/youtube/answer/76187?hl=en</u>
- TikTok account recovery instructions: <u>https://support.tiktok.com/en/log-in-</u> <u>troubleshoot/log-in/my-account-has-been-hacked</u>
- Twitter/X account recover: <u>https://help.x.com/en/safety-and-security/x-account-</u> <u>compromised</u>
- Bluesky account recovery: <u>https://bsky.social/about/support/tos#who-can-use</u>

8.5. Containment and Eradication

8.5.1. Contain the Threat

- **Suspend Activity:** Temporarily suspend or limit account activity to prevent further unauthorized actions until the threat is contained.
- **Remove Malicious Content:** Delete any unauthorized posts, messages, or comments that may harm the organization's reputation or mislead followers.
- **Assess Impact:** Determine the extent of the attack, including whether sensitive data or customer information has been exposed.

8.5.2. Eradicate the Threat

- **Investigate the Incident:** Identify how the attack occurred, whether through phishing, weak passwords, or compromised third-party apps.
- **Patch Vulnerabilities:** Address any vulnerabilities identified during the investigation, such as insecure passwords or outdated security settings.
- Scan for Malware: If the attack involved malicious links or software, scan connected devices and networks for malware and remove any threats.

8.6. Recovery and Communication

8.6.1. System Recovery

- **Restore Normal Operations:** Once the account is secure, restore normal posting and engagement activities.
- **Monitor Activity:** Closely monitor the account for any signs of residual threat activity or further unauthorized access attempts.

8.6.2. Internal Communication

- **Debrief Teams:** Provide a detailed debrief to all relevant teams, including IT, social media, and communications, about the incident and recovery steps.
- **Review Access Control:** Reassess who has access to the account and ensure that only necessary personnel have administrative privileges.

8.6.3. External Communication



- **Inform Followers:** If necessary, inform the account's followers of the incident and reassure them that the situation is under control. Provide guidance if they were affected (e.g., exposed to phishing links).
- **Public Statement:** Prepare and release a public statement through appropriate channels, acknowledging the incident and outlining the steps taken to secure the account and prevent future occurrences.
- **Notify Authorities:** If the attack involved significant data breaches or illegal activities, notify relevant law enforcement agencies or regulatory bodies.

9. Incident Response Strategy for Social Media Account Dogpiling

9.1. Purpose

This strategy outlines the steps to be taken when an organization's social media account or a staff member's account is targeted by a dogpiling attack. Dogpiling refers to a coordinated or spontaneous online harassment campaign where numerous users post negative, abusive, or harmful comments in a short period. The goal is to minimize harm, protect affected individuals, and manage the organization's reputation.

9.2. Scope

This strategy applies to all social media accounts managed by the organization, as well as personal accounts of employees when the attack is related to their professional role or association with the organization.

9.3. Incident Detection

9.3.1. Indicators of Dogpiling

- Sudden influx of negative, abusive, or harassing comments, mentions, or direct messages.
- A significant increase in notifications across one or more social media platforms.
- Coordinated attacks from multiple accounts, often with similar messaging or hashtags.
- Use of inflammatory language, threats, or hate speech directed at the organization or specific individuals.

9.4. Immediate Response Steps

9.4.1. Employee Actions



- **Do Not Engage:** Employees should avoid responding to or engaging with individuals participating in the dogpiling attack.
- **Report Immediately:** Notify the social media team or designated incident response team as soon as the attack is detected.
- **Preserve Evidence:** Take screenshots and document the nature of the attack, including usernames, comments, and timestamps, without responding to the attackers.

9.4.2. Social Media Team/Incident Response Team Actions

• Assess the Situation:

- **Content Review:** Review the content and scale of the dogpiling to assess its severity and potential impact on the organization or individuals.
- **Source Identification:** Identify whether the attack is organic (spontaneous) or coordinated, and note any specific groups or accounts leading the attack.
- Implement Defensive Measures:
 - **Content Moderation:** Immediately moderate harmful content by hiding, deleting, or reporting comments and posts that violate platform policies.
 - Adjust Account Settings: Temporarily adjust account settings to limit further damage. This may include restricting comments, turning off direct messaging, or enabling additional content moderation filters.
 - **Block and Report:** Block and report accounts that are primarily responsible for the attack, particularly those engaging in hate speech or threats.

9.5. Containment and Mitigation

9.5.1. Contain the Threat

• Secure Social Media Accounts: Ensure that all social media accounts are secure, with strong passwords and multi-factor authentication enabled. Consider temporarily limiting access to account managers only.

9.5.2. Mitigate Impact on Individuals

- Provide Support:
 - **Emotional Support:** Offer counseling or support services to employees affected by the attack.
 - **Temporary Social Media Break:** If the attack is particularly severe, consider temporarily taking down affected accounts or advising affected individuals to take a break from social media.
 - Remove targeted individuals from sensitive communications until situation settles
- Public Communication:
 - Statement of Response: Prepare a carefully worded public statement if necessary, acknowledging the situation, condemning harassment, and emphasizing the organization's values. Avoid escalating the situation or engaging directly with attackers.



• **Monitor Public Sentiment:** Continuously monitor public sentiment and media coverage to adapt the response strategy as needed.

9.6. Recovery and Communication

9.6.1. Account Recovery

- **Restore Normal Operations:** Once the attack subsides, gradually restore normal account settings and continue to monitor for any resurgence of the attack.
- **Content Review:** Review all content and communication during the attack to ensure that no harmful posts remain visible and that all inappropriate comments have been addressed.

9.6.2. Internal Communication

• **Brief Employees:** Provide a briefing to employees, especially those involved in managing social media accounts, on the incident and the steps taken. Offer guidance on handling similar incidents in the future.

9.6.3. External Communication

- **Proactive Engagement:** If consensus is reached internally then consider engaging with followers and the community to reaffirm the organization's commitment to its values and to support positive online interaction.
- **Stakeholder Communication:** If the incident has broader implications, communicate with key external stakeholders, such as partners or clients, to reassure them of the organization's stability and approach to managing online threats.

10. Website Attack Incident Response Strategy

10.1. Purpose

This strategy outlines the steps to be taken when an organization's website is attacked or compromised. The objective is to minimize damage, restore normal operations, and prevent future incidents.

10.2. Scope

This strategy applies to all websites owned or operated by the organization, including associated web applications, databases, and servers. It covers a range of potential attacks, including but not limited to Distributed Denial of Service (DDoS) attacks, website defacement, malware injection, SQL injection, and unauthorized access.



10.3. Incident Detection

10.3.1. Indicators of an Attack

- Unusual spikes in traffic, especially from unknown sources or unusual geolocations.
- Website defacement, including unauthorized changes to content, images, or layout.
- Slow website performance or downtime.
- Unauthorized redirects to other websites.
- Detection of malware or malicious scripts on the website.
- Alerts from security tools about suspicious activities, such as multiple failed login attempts, unauthorized access, or changes to files.

10.4. Immediate Response Steps

10.4.1. Employee/Administrator Actions

- **Report Immediately:** If you suspect that the website is under attack, report the incident to the IT department or the designated website security team immediately.
- **Do Not Modify:** Avoid making any changes to the website until the security team has been notified and has taken control of the situation.
- **Collect Information:** Document any suspicious activities, including screenshots, error messages, and any relevant logs.

10.4.2. IT Department/Website Security Team Actions

- Isolate the Threat:
 - **Take the Website Offline:** If necessary, take the website offline temporarily to prevent further damage or data loss.
 - **Restrict Access:** Limit access to the website and associated systems to essential personnel only.
 - **Identify the Attack:** Use monitoring tools and logs to identify the type of attack and the entry point used by the attackers.
- Communicate Internally:
 - Inform relevant stakeholders, including executive leadership, the communications team, and legal counsel, about the incident and initial steps taken.
 - Coordinate with the public relations team to prepare for potential external communication if the incident is severe.

10.5. Containment and Eradication

10.5.1. Contain the Threat

• **Apply Temporary Fixes:** Implement temporary measures, such as blocking malicious IP addresses, disabling vulnerable features, or applying patches to prevent the attack from spreading or escalating.



- **Secure Backups:** Ensure that backups of the website and its data are secure and not compromised. Prepare to restore from backups if necessary.
- **Preserve Evidence:** Preserve logs, snapshots, and any other evidence that might be needed for a forensic investigation or legal action.

10.5.2. Eradicate the Threat

- **Remove Malicious Code:** Identify and remove any malicious code, scripts, or files that were introduced during the attack.
- **Patch Vulnerabilities:** Identify and patch any vulnerabilities that were exploited, such as outdated software, insecure configurations, or weak passwords.
- **Reset Credentials:** Reset all credentials associated with the website, including administrative passwords, database passwords, and API keys, and enforce stronger password policies.

10.6. Recovery and Communication

10.6.1. System Recovery

- **Restore Services:** Once the website is secure, restore it to normal operation, using clean backups if necessary.
- **Monitor for Further Activity:** Monitor the website closely for any signs of continued malicious activity, unauthorized access attempts, or other anomalies.

10.6.2. Internal Communication

- **Debrief Teams:** Provide a detailed debrief to all relevant teams, including IT, communications, and leadership, about the incident and the steps taken to secure the website.
- **Review Access Controls:** Review and update access controls, ensuring that only authorized personnel have the necessary permissions.

10.6.3. External Communication

- **Inform Users:** If user data was compromised or the attack had a significant impact, inform affected users promptly and provide guidance on any actions they should take (e.g., changing passwords).
- **Public Statement:** Prepare and release a public statement, if necessary, acknowledging the incident and explaining the steps taken to resolve it and prevent future occurrences.
- **Notify Authorities:** If the attack involved data breaches or illegal activities, notify the relevant law enforcement agencies or regulatory bodies.

Recommendation: Regularly backup website data and store copies in a secure location, such as an external server or cloud storage. Additionally, consider archiving versions of the site using the Internet Archive or similar services to preserve critical content. These backups will help restore the website quickly in the event of an attack, defacement, or data loss.



11. Incident Response Strategy for Doxxing of an Organizational Member

11.1. Purpose

This strategy outlines the response plan for when an executive director or any leadership member of the organization has their personal information leaked online, also known as doxxing. The objective is to protect the individual's safety, mitigate potential damage to the organization, and manage the situation effectively.

11.2. Scope

This strategy applies to incidents involving the unauthorized disclosure of personal information of any member of the organization's leadership team. This includes information such as home addresses, phone numbers, email addresses, family details, and other sensitive personal data.

11.3. Incident Detection

11.3.1. Indicators of Doxxing

- Discovery of personal information posted on social media, forums, or other websites.
- Receipt of threatening or harassing communications directed at the executive or their family members.
- Sudden increase in unwanted contacts, such as phone calls, emails, or visits to the executive's home.
- Reports from colleagues, media, or law enforcement about the exposure of the executive's personal information.

11.3.2. Doxxing Early Warning System

• Set up Google Alerts for leadership members, executives, and official organizational accounts (including social media handles) to monitor potential doxxing threats. General members can set up alerts for their own individual accounts separately.

11.4. Immediate Response Steps

11.4.1. Executive/Leadership Actions

• **Report Immediately:** The affected executive or leadership member should immediately report the doxxing incident to the organization's security team or designated point of contact.



- Limit Exposure: Refrain from engaging with or responding to any communications or threats received as a result of the doxxing.
- **Document the Incident:** Keep records of all instances of harassment, including screenshots, emails, messages, and any other relevant evidence.

11.4.2. Security/IT Team Actions

- Verify the Incident:
 - **Assess the Information:** Verify the accuracy and scope of the leaked information and determine where it was posted.
- Secure the Individual:
 - Personal Security: If necessary, arrange for physical security measures for the executive, such as increased home security, temporary relocation, or private security services.
 - **Cybersecurity Measures:** Assist the individual in securing their personal digital accounts, including changing passwords, enabling multi-factor authentication, and reviewing account activity.
- Mitigate Online Exposure:
 - **Request Removal:** Contact website administrators, social media platforms, and search engines to request the removal of the leaked information.
 - **Legal Action:** Explore legal options, such as cease and desist orders, to compel the removal of personal information and to prevent further dissemination.
 - **Decide when necessary to notify Law Enforcement:** Contact local law enforcement to report the doxxing incident and seek their assistance if there is a threat to the individual's safety.

11.5. Containment and Mitigation

11.5.1. Contain the Spread

- **Suppress Search Results:** Work with legal and public relations teams to suppress search results that reveal the doxxed information, using tools like Google's removal requests.
- **Public Relations Response:** Prepare a public relations response if necessary to address any media coverage or public awareness of the incident. This should aim to protect the individual's privacy while maintaining the organization's reputation.

11.5.2. Support for the Affected Individual

- **Emotional Support:** Provide access to counseling services or support resources for the affected executive and their family members to help manage the emotional impact of the doxxing.
- **Ongoing Monitoring:** Continue monitoring online platforms for further leaks or threats, and keep the individual informed of any developments.



11.6. Recovery and Communication

11.6.1. Internal Communication

- **Inform Leadership:** Notify the organization's executive team and relevant stakeholders about the incident, the steps taken to protect the individual, and any ongoing risks.
- Limit Internal Exposure: Ensure that the incident is communicated on a need-to-know basis to avoid unnecessary spread of sensitive information within the organization.

11.6.2. External Communication

- **Manage Public Narrative:** If the incident becomes public, manage external communications carefully to protect the individual's privacy and the organization's reputation.
- **Stakeholder Communication:** Communicate with key external stakeholders, such as partners and clients, to reassure them of the organization's continued stability and security.

12. Self-Care Recommendations for After Being Doxxed

Being doxxed—having personal information exposed publicly without consent—can be a distressing experience. It's important to prioritize self-care and take steps to address both emotional and practical concerns. Here are some self-care recommendations for managing the aftermath of being doxxed:

12.1. Emotional Self-Care

12.1.1. Acknowledge Your Feelings

- Validate Your Emotions: It's normal to feel a range of emotions, including anger, fear, or anxiety. Allow yourself to feel and express these emotions without judgment.
- Seek Support: Talk to trusted friends, family members, or a mental health professional about your experience. Sharing your feelings can help alleviate some of the emotional burden.

12.1.2. Practice Stress-Reduction Techniques

- **Mindfulness and Relaxation:** Engage in mindfulness practices, such as meditation or deep-breathing exercises, to help manage stress and anxiety.
- **Physical Activity:** Regular exercise can help reduce stress and improve overall wellbeing. Activities like walking, yoga, or other forms of exercise can be beneficial.



12.1.3. Establish Boundaries

- Limit Exposure: If the doxxing incident has resulted in negative online interactions, consider taking a break from social media or limiting your exposure to distressing content.
- **Create Safe Spaces:** Engage in activities and spend time in environments that make you feel safe and supported.

12.2. Practical Self-Care

12.2.1. Address Security Concerns

- Secure Your Online Accounts: Change passwords for all online accounts, and enable multi-factor authentication where possible. Review privacy settings and restrict access to personal information.
- **Monitor Your Accounts:** Keep an eye on your financial and social media accounts for any unusual activity or signs of misuse.

12.2.2. Protect Personal Information

- **Update Personal Details:** If your personal information, such as your address or phone number, has been exposed, consider updating or securing these details. Contact relevant services to request updates or additional security measures if necessary.
- **Consult Professionals:** Consider seeking advice from cybersecurity professionals or legal experts to understand how to further protect yourself and address any legal implications.

12.3. Legal and Administrative Steps

12.3.1. Report the Incident

- **Notify Authorities:** Report the doxxing to local law enforcement if you feel threatened or if there are legal concerns. Provide them with any relevant information and evidence.
- **Contact Platforms:** Report the incident to social media platforms or websites where your information was exposed. Request that they take down any harmful or unauthorized content.

12.3.2. Document the Incident

• Keep Records: Document all instances of harassment or misuse of your personal information. Keep screenshots, emails, and other relevant evidence for future reference or potential legal action.

12.4. Long-Term Self-Care



12.4.1. Build a Support Network

- Seek Community Support: Connect with support groups or organizations that specialize in online harassment or doxxing. They can offer guidance, resources, and a sense of community.
- **Maintain Relationships:** Stay connected with friends and family who can provide emotional support and practical assistance during this time.

12.4.2. Engage in Positive Activities

- **Pursue Hobbies:** Engage in activities that bring you joy and fulfillment. Hobbies and interests can provide a healthy distraction and improve your overall mood.
- Focus on Self-Care: Prioritize activities that contribute to your well-being, such as getting adequate rest, maintaining a healthy diet, and engaging in activities that promote relaxation and happiness.

12.5. Professional Help

12.5.1. Seek Therapy or Counseling

• **Mental Health Support:** Consider working with a therapist or counselor who can help you process the trauma and develop coping strategies. They can provide a safe space to explore your feelings and work through the impact of the incident.

12.5.2. Legal Consultation

• **Legal Advice:** If you are facing ongoing harassment or have concerns about legal implications, consult with a legal professional who specializes in privacy or cyber law.

Important Note: Each individual's experience with doxxing is unique, and self-care needs may vary. It's essential to tailor these recommendations to your specific situation and seek professional advice if needed.

By taking these steps, you can better manage the emotional and practical challenges following a doxxing incident, and work towards reclaiming a sense of safety and well-being.

References:

https://onlineviolenceresponsehub.org/wp-content/uploads/2024/01/CAOV-MAPPING-REPORT-2024.pdf



References and Resources:

1Password. (n.d.). *Password manager* & *extended access management*. <u>https://1password.com/</u>

Amazon. (n.d.). *Cybersecurity awareness training.* https://learnsecurity.amazon.com/en/index.html

Bitdefender. (n.d.). *Bitdefender free antivirus software for windows*. <u>https://www.bitdefender.com/en-us/consumer/free-antivirus</u>

Bluesky Social. (2025, February 7). *Terms of service*. <u>https://bsky.social/about/support/tos#who-can-use</u>

Chrome Web Store. (n.d.). *AdBlock - block ads across the web*. <u>https://chromewebstore.google.com/detail/adblock-%E2%80%94-block-ads-acros/gighmmpiobklfepjocnamgkkbiglidom</u>

Chrome Web Store. (n.d.). *Adblock Plus - Free ad blocker*. <u>https://chromewebstore.google.com/detail/adblock-plus-free-ad-bloc/cfhdojbkjhnklbpkdaibdccddilifddb</u>

Cook, S. (2021, November 24). *What is vishing? How to recognize and avoid phishing scams*. Comparitech. <u>https://www.comparitech.com/blog/information-security/what-is-vishing-how-to-avoid/</u>

CyberGhost. (n.d.). *Fast, secure* & *anonymous vpn service* | *CyberGhost vpn.* <u>https://www.cyberghostvpn.com/</u>

Dashlane. (n.d.). *Password manager for mobile, home and business*. <u>https://www.dashlane.com/</u>

Duo. (n.d.). Identity security, mfa & ssO | Duo security. https://duo.com/

Facebook. (n.d.). *Recover a hacked Facebook account.* https://www.facebook.com/help/203305893040179

Gonzalez, C. (2023, May). *Coalition against online violence: Mapping report 2024*. International Women's Media Foundation. <u>https://onlineviolenceresponsehub.org/wp-</u> content/uploads/2024/01/CAOV-MAPPING-REPORT-2024.pdf

Google. (n.d.). *Get verification codes with Google authenticator codes*. Google Support. <u>https://support.google.com/accounts/answer/1066447?hl=en&co=GENIE.Platform%3DAndroid</u>



Google. (n.d.). *Recover a hacked YouTube channel*. https://support.google.com/youtube/answer/76187?hl=en&authuser=1

Google. (n.d.). *Simpler sign-in, safer passwords*. Google Password Manager. <u>https://passwords.google/</u>

Google. (n.d.). *Titan security key*. Google Cloud. https://cloud.google.com/security/products/titan-security-key

Government of Canada. (2021, October 27). *VPNs*. <u>https://www.getcybersafe.gc.ca/en/secure-your-connections/vpns</u>

Government of Canada. (2021, November 3). *Real examples of fake emails*. <u>https://www.getcybersafe.gc.ca/en/resources/real-examples-fake-emails</u>

Government of Canada. (2022, July 25). *What is voice phishing (vishing)? - ISTAP.00.102.*. <u>https://www.cyber.gc.ca/en/what-voice-phishing-vishing-itsap00102</u>

Government of Canada. (2023, November 21). *What is vishing*?. <u>https://www.getcybersafe.gc.ca/en/blogs/what-vishing</u>

Hrynchuk, S. (2020, August 12). *E-Mail money transfer*. Scam Detector. <u>https://www.scam-detector.com/article/e-mail-money-transfer/</u>

InfoSec Institute. (n.d.). *Work bytes: Award-winning engaging cybersecurity training.* <u>https://www.infosecinstitute.com/iq/work-bytes/</u>

Instagram. (n.d.). *If you think your Instagram account has been hacked*. <u>https://help.instagram.com/149494825257596</u>

Keeper Security. (n.d.). *Keeper Security: Password management and privileged access management (PAM) solution*. <u>https://www.keepersecurity.com/</u>

Kim, J. (2024, June 24). *How many characters should my password be?*. Keeper Security. <u>https://www.keepersecurity.com/blog/2024/06/24/how-many-characters-should-my-password-be/</u>

KnowBe4. (n.d.). *KnowBe4 security awareness training.* https://www.knowbe4.com/products/security-awareness-training

Kozinski, K. & Kapur, N. (2020, February 27). *How to dox yourself on the internet*. New York Times. <u>https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954</u>

LinkedIn. (n.d.). *Build your cybersecurity awareness skills.* https://www.linkedin.com/learning/paths/build-your-cybersecurity-awareness-skills



LinkedIn. (2025, March). *Verify your identity to recover account access.* <u>https://www.linkedin.com/help/linkedin/answer/a1342692</u>

McAfee. (n.d.). *McAfee antivirus software 2025 Anti-virus free download.* <u>https://www.mcafee.com/en-us/antivirus.html</u>

McGowan, E. (2024, February 20). *What is vishing? Tips to spot and avoid voice phishing scams*. Norton. <u>https://us.norton.com/blog/online-scams/vishing</u>

Microsoft. (n.d.). *About Microsoft authenticator*. Microsoft Support. <u>https://support.microsoft.com/en-us/account-billing/about-microsoft-authenticator-9783c865-0308-42fb-a519-8cf666fe0acc</u>

Microsoft Edge. (n.d.). AdGuard AdBlocker. https://microsoftedge.microsoft.com/addons/detail/adguardadblocker/pdffkfellgipmhklpdmokmckkkfcopbh

Mozilla. (n.d.). *AdBlocker Ultimate*. Firefox Browser Add-ons. <u>https://addons.mozilla.org/en-US/firefox/addon/adblocker-ultimate/</u>

Mozilla. (n.d.). *Get Mozilla vpn - Mozilla (US)*. Firefox Browser Add-ons. <u>https://www.mozilla.org/en-US/products/vpn/</u>

Mozilla. (n.d.). *uBlock Origin.* Firefox Browser Add-ons. <u>https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/</u>

National Institute of Standards and Technology. (n.d.). *Free and low cost online cybersecurity learning content*. <u>https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content</u>

Norton. (n.d.). *Official site* | *Norton*[™] - *Antivirus* & anti malware software. <u>https://ca.norton.com/?lsModal=1#</u>

PEN America. (n.d.). Digital safety snacks. https://pen.org/digital-safety-snacks/

Proton. (n.d.). The best VPN for speed and security. Proton VPN. https://protonvpn.com/

r/VPN [paperplans5]. (2021, March 17). *VPN comparison table* [Online forum post]. Reddit. <u>https://www.reddit.com/r/VPN/comments/m736zt/vpn_comparison_table/</u>

RAINN. (n.d.). *How to filter, block, and report harmful content on social media.* <u>https://rainn.org/articles/how-filter-block-and-report-harmful-content-social-media</u>



Right to Be. (n.d.). *How to strengthen your digital security*. <u>https://righttobe.org/guides/how-to-strengthen-your-digital-security/</u>

Right to Be. (n.d.). *Prepare your organization against online harassment.* https://righttobe.org/guides/fortify-your-organization-against-online-harassment/

Site Admin. (2022, September 26). *Fake invoice phishing scams*. Information Technology Lawrence Berkeley National Laboratory. <u>https://it.lbl.gov/fake-invoice-phishing-scams/</u>

Tech Safety Canada. (n.d.). Home | Tech safety Canada. https://techsafety.ca/

TikTok. (n.d.). *My account has been hacked*. <u>https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked</u>

UPS. (2025). *Protect yourself from fraud and scams*. UPS. https://www.ups.com/ca/en/support/shipping-support/legal-terms-conditions/fight-fraud.page

X. (n.d.). *Help with my compromised account*. X Help Center. <u>https://help.x.com/en/safety-and-security/x-account-compromised</u>

Yaqub, O. (2023, May 10). *IslamicFamily cybersecurity policy*. Notion. <u>https://islamicfamily.notion.site/IslamicFamily-Cybersecurity-Policy-</u> <u>c57681d4bf90456b9b7eb013a483fbb5</u>