

Course Outline & Learning Options

SEC-104 – Online Safety, Password Security and Identity Protection

Practical skills to protect accounts, personal information, and digital identity

Course Information

Course Title	Online Safety, Password Security and Identity Protection
Course Number	SEC-104
Learning Series	Digital Safety and Everyday Technology Skills
Prerequisites	Basic comfort using a computer, smartphone, tablet, or email account. No cybersecurity experience required.
Duration	Approximately 4.5 hours, including instruction, guided exercises, discussion, review, and questions
Delivery Format	- Self-Directed Learning - Live Online Workshop - On-Site Group Training - One-on-One Coaching
Languages	English, French, Bilingual
Pricing	Available upon request based on delivery format, group size, customization, and printed materials.
Author	MCT Office Services

Course Description

This beginner-friendly course helps participants build confidence using the internet safely, creating stronger passwords and passphrases, recognizing common scams, protecting personal information, and responding calmly if an account or identity concern occurs. The course uses plain language, demonstrations, guided practice, and everyday examples suitable for individuals, seniors, community groups, professionals, and small business owners.

Learning Outcome: Participants will be able to apply practical online safety habits to protect their accounts, passwords, personal information, and digital identity.

Learning Objectives

By the end of this course, participants will be able to:

- Create stronger passwords and passphrases using current best practices.
- Use password managers and multi-factor authentication more confidently.
- Recognize phishing, smishing, suspicious links, unsafe downloads, AI-generated pictures and posts, deepfakes, and common online scams.
- Take practical steps to reduce identity theft risk and respond if personal information is exposed.

Target Audience

This course is designed for:

- Administrative professionals
- Beginners
- Community groups
- Individuals
- Lifelong learners
- Professionals
- Seniors
- Small business owners
- Students

Customization Options

- Duration may be adjusted.
- Content may be customized
- Additional demonstrations
- Industry-specific examples
- English, French, or bilingual delivery available
- Printed participant guides and reference materials available
- Follow-up coaching and additional workshops available.

Learning Activities

- Knowledge checks on safe and unsafe online behaviours
- Guided password and passphrase creation exercises
- Real-world scam and phishing recognition scenarios
- AI-generated images, posts, deepfakes, and scam-recognition activities
- Hands-on account security checklist activities
- Personal online safety self-assessment

Module Breakdown

MODULE 1 – UNDERSTANDING ONLINE RISKS

Estimated time: 30 minutes, including discussion and threat-recognition exercise

Key Topics:

- Common online threats and how they occur
- Phishing emails and fraudulent text messages
- Fake websites, advertisements, pop-ups, and login pages
- Social media scams and account impersonation
- Fraudulent phone calls and technical-support scams
- Identity theft and misuse of personal information
- Data breaches and exposed passwords
- Warning signs that an account or device may be compromised
- The importance of pausing and verifying before responding, clicking, downloading, or sharing information

Exercises:

- Review several realistic online situations and identify the type of risk involved.
- Sort examples into safe, suspicious, and unsafe categories.
- Discuss what participants should pause to verify before responding or clicking.

MODULE 2 – CREATING AND MANAGING STRONG PASSWORDS

Estimated time: 35 minutes, including passphrase creation and password-management exercise

Key Topics:

- Characteristics of a strong password
- Using long, memorable passphrases
- Creating a different password for every important account
- Risks associated with reusing passwords
- Personal information that should not be included in passwords
- Avoiding predictable words, dates, names, and number patterns
- Changing default passwords on devices and online accounts
- When a password should be changed
- Storing passwords securely
- Benefits and limitations of password managers
- Selecting and protecting a password manager
- Avoiding passwords stored in unsecured notebooks, documents, emails, or contact lists

Exercises:

- Create sample passphrases using a safe structure without using personal information.
- Identify weak, reused, or predictable passwords in sample examples.
- Discuss how participants would decide which accounts should be updated first.

MODULE 3 – PROTECTING ACCOUNTS WITH MULTI-FACTOR AUTHENTICATION

Estimated time: 30 minutes, including MFA prioritization and verification-code safety exercise

Key Topics:

- What multi-factor authentication is and how it protects an account
- The difference between a password and an additional verification method
- Common verification methods: authenticator applications, security keys, text-message codes, email codes, and biometric verification

- Which accounts should be protected first
- Enabling multi-factor authentication on email, banking, social media, cloud storage, and government accounts
- Protecting recovery codes and backup verification methods
- Recognizing fraudulent requests for verification codes
- Understanding that legitimate organizations generally do not ask customers to disclose security codes
- Reviewing account recovery information regularly

Exercises:

- Rank account types by priority for multi-factor authentication.
- Review examples of legitimate and suspicious verification-code requests.
- Create a simple backup-code storage plan.

Module 4 – Recognizing Scams and Phishing Attempts

Estimated time: 40 minutes, including phishing-analysis and Stop, Check, Verify, Decide practice

Key Topics:

- Common characteristics of fraudulent messages
- Unexpected requests for payment, passwords, codes, or personal information
- Messages that create urgency, fear, secrecy, or pressure
- Offers, prizes, refunds, and investment opportunities that appear too good to be true
- Suspicious sender names, email addresses, telephone numbers, and website addresses
- Spelling, formatting, branding, and language inconsistencies
- Links and attachments that should not be opened
- QR-code scams and shortened web links
- Fraudulent invoices, delivery notices, account alerts, and subscription-renewal messages
- Family-emergency and government-impersonation scams
- Verifying a request using independently obtained contact information
- Reporting, blocking, and deleting suspicious messages
- Using the Stop, Check, Verify, Decide method before taking action

Exercises:

- Analyze sample emails, text messages, invoices, alerts, and social media messages for warning signs.
- Practise applying the Stop, Check, Verify, Decide method to several scenarios.
- Identify the safest way to verify a request without using the contact details in the suspicious message.

Module 5 – Protecting Personal Information and Identity

Estimated time: 35 minutes, including privacy-settings and personal-information review exercise

Key Topics:

- Types of personal information targeted by criminals
- Protecting birth dates, addresses, account numbers, identification documents, and financial information
- Limiting the personal information shared on social media
- Reviewing privacy and security settings
- Recognizing oversharing and information that can be used to answer security questions
- Protecting personal information when shopping or banking online
- Checking that websites are legitimate before entering information

- Understanding the limits of the padlock symbol and HTTPS
- Avoiding sensitive transactions on unsecured public Wi-Fi
- Using secure home Wi-Fi and changing router default credentials
- Keeping devices, applications, browsers, and security software updated
- Locking devices with a password, PIN, fingerprint, or facial recognition
- Safely disposing of documents and old electronic devices
- Monitoring financial statements, credit reports, and account activity for unfamiliar transactions

Exercises:

- Complete a personal-information exposure review using a checklist.
- Identify information that should be removed, limited, or protected more carefully online.
- Discuss privacy settings and safer practices for shopping, banking, social media, and public Wi-Fi.

Module 6 – Recognizing AI-Generated Pictures, Posts, Deepfakes, and Scams

Estimated time: 35 minutes, including visual-analysis practice and verification workflow exercise

Key Topics:

- What AI-generated pictures, posts, videos, and voice messages can look and sound like
- Why single “tells” are not reliable and why several clues should be considered together
- Visual warning signs such as unusual lighting, inconsistent shadows, distorted backgrounds, mismatched reflections, unnatural skin or hair texture, and odd details in hands, teeth, glasses, jewellery, signs, or logos
- Social media warning signs such as sensational claims, emotional pressure, copied posts, fake giveaways, investment promotions, miracle products, and impersonated public figures or organizations
- Deepfake video and voice-cloning risks, including fake endorsements, fake emergency requests, and fraudulent authorization requests
- Checking the source, date, account history, web address, and whether the same claim appears on trusted sources
- Using reverse image search, official websites, independent contact information, and trusted reporting channels to verify content
- Understanding that AI-detection tools can help but may be wrong, so decisions should not rely on one tool alone
- Reporting suspicious AI-generated scams, blocking fraudulent accounts, and avoiding sharing unverified content

Exercises:

- Compare sample images and posts to identify possible AI-generation clues and missing context.
- Apply a “Pause, Inspect, Verify, Report” checklist to AI-generated scam scenarios.
- Practise verifying a suspicious image, social media post, or video claim using independent sources rather than links provided in the message.

Module 7 – Responding to a Security Incident

Estimated time: 35 minutes, including incident-response scenario and personal response plan exercise

Key Topics:

- Immediate actions if a suspicious link or attachment has been opened
- Disconnecting a device when malicious activity is suspected

- Changing an exposed password from a trusted device
- Changing reused passwords on other accounts
- Signing out of active sessions and removing unfamiliar devices
- Contacting the bank or credit-card company about suspicious transactions
- Contacting the affected service through its official website or telephone number
- Reporting fraud to the appropriate organization or authority
- Preserving emails, messages, receipts, screenshots, and other evidence
- Checking account recovery details and forwarding rules
- Running device security scans and installing updates
- Monitoring accounts and credit reports after an incident
- Informing contacts if an email or social media account has been used to send fraudulent messages
- Creating a personal response plan and keeping important contact information accessible

Exercises:

- Work through a compromised-account scenario and identify the first actions to take.
- Build a simple personal response plan with key contacts, recovery steps, and reporting options.
- Discuss what evidence should be preserved and when professional support may be needed.

Module 8 – Practical Review and Questions

Estimated time: 35 minutes, including review activities, action planning, and questions

Key Topics:

- Review examples of legitimate and suspicious messages
- Identify warning signs in a sample phishing attempt
- Review AI-generated pictures, posts, videos, or voice-message examples for warning signs and missing context
- Practise creating a strong passphrase
- Identify the most important accounts to protect with multi-factor authentication
- Complete a short personal online-safety review
- Select two or three security improvements to implement immediately
- Ask questions about individual online-safety concerns

Exercises:

- Complete a final online-safety checklist.
- Select two or three immediate security improvements to complete after the session.
- Share remaining questions and identify next steps for continued support.

Digital Resources Included

Participants receive the following digital learning resources to support learning during and after the course:

- Digital Participant Guide (where applicable)
- Exercise Booklet (where applicable)
- Online Safety Reference Card
- Strong Passwords and Passphrases Reference Card
- Scam and Phishing Recognition Checklist

- Personal Online Safety Checklist
- Security Incident Response Checklist
- Additional Learning Resources
- Certificate of Participation (available upon request)

Available Online Safety, Password Security, and Identity Protection Resources

The following public resources may help participants continue learning, verify suspicious situations, and find trusted reporting options after the course:

Online Safety and Scam Awareness

- Get Cyber Safe – Plain-language cyber safety tips for Canadians, including account protection, device safety, scams, phishing, passphrases, password managers, and multi-factor authentication. www.getcybersafe.gc.ca
- Canadian Centre for Cyber Security – Information for Individuals – Guidance on cyber safety, phishing, identity and passwords, artificial intelligence, malware, ransomware, and incident response. www.cyber.gc.ca/en/individuals
- Government of Canada – Scams and Fraud – Guidance on recognizing scams, AI-enabled deception, government impersonation, disinformation, and where to report concerns. www.canada.ca/en/revenue-agency/campaigns/fraud-scams.html

Password Security and Account Protection

- Government of Canada – Guideline on Password Security – Best-practice guidance on passwords, passphrases, authentication, and password-manager considerations. www.canada.ca/en/government/system/digital-government/online-security-privacy/identity-credential-access-management/password-guidance.html
- Canadian Centre for Cyber Security – Password Managers: Security Tips – Practical guidance on choosing and using password managers safely. www.cyber.gc.ca/en/guidance/password-managers-security-itsap30025
- Get Cyber Safe – Password Managers – Beginner-friendly resource explaining how password managers help create, store, and manage unique passwords. www.getcybersafe.gc.ca/en/resources/password-managers
- Canadian Centre for Cyber Security – Phishing-Resistant Multi-Factor Authentication – Advanced guidance for organizations that want stronger protection against modern phishing attacks. www.cyber.gc.ca/en/guidance/defending-against-adversary-middle-threats-phishing-resistant-multi-factor-authentication-itsm30031

Identity Protection and Privacy

- Canadian Centre for Cyber Security – Protecting Yourself from Identity Theft Online – Guidance on digital identity, personal information risks, phishing, data breaches, and steps to protect your identity. www.cyber.gc.ca/en/guidance/protecting-yourself-identity-theft-online-itsap00033
- Office of the Privacy Commissioner of Canada – Identity Theft – Practical information on reducing identity-theft risk and what to do if personal information is misused. www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/

- Office of the Privacy Commissioner of Canada – For Individuals – Privacy rights, online privacy guidance, breach notifications, Social Insurance Number protection, and resources for seniors. www.priv.gc.ca/en/for-individuals/

Reporting Fraud, Cybercrime, or Identity Theft

- Canadian Anti-Fraud Centre – Main Resource Hub – Information on current frauds affecting Canadians, fraud prevention, identity theft, and victim support. www.antifraudcentre-centreantifraude.ca/index-eng.htm
- Canadian Anti-Fraud Centre – Report Fraud and Cybercrime – Online and phone reporting options for victims and witnesses of fraud or cybercrime. www.antifraudcentre-centreantifraude.ca/report-signalez-eng.htm
- Report Cybercrime and Fraud Portal – Direct online reporting portal for fraud and cybercrime in Canada. report.antifraudcentre.ca
- Canada Revenue Agency – Report a Scam or Identity Theft – Steps to take if a CRA account may be compromised or suspicious activity is noticed. www.canada.ca/en/revenue-agency/corporate/scams-fraud/report-scam.html

Note:

Optional printed participant materials, including printed participant guides and laminated reference resources, are available at an additional cost. Please refer to the current MCT Course Options & Pricing Guide for details.

Upon Completion

Upon completion of this course, participants will be able to use practical online-safety habits to protect accounts and personal information, recognize common scams and AI-generated deceptive content, verify suspicious requests, and respond more confidently to security concerns.

Online Safety Reminder

Participants should protect personal information, verify suspicious requests independently, use professional judgment, and seek qualified technical, financial, or legal assistance when necessary.



**Helping you work more efficiently, stay organized,
and use technology with confidence.**

About MCT Office Services

MCT Office Services provides friendly, patient, and practical support for individuals, seniors, community groups, and small businesses that need help with technology, paperwork, organization, and digital learning.

- Technology support and troubleshooting
- Forms, paperwork, and online applications
- Document creation, formatting, and organization.
- Guidance with digital tools, including beginner-friendly AI support.
- Administrative and organizational support
- One-on-one coaching and small-group workshops

No memberships. No contracts. Just practical help when you need it.

Camylle Tremblay
MCT Office Services
Orléans, Ontario

Questions?
Contact MCT Office Services for a free
consultation.

Email:
admin@mctofficeservices.com
Phone: (343) 887-6701
Web: www.mctofficeservices.ca

SEC-104
Version 1.0
August 2026