Lock the Door to Your Data

OBIAA™

GRAND ERIE BUSINESS CENTRE

DIGITAL MAIN ST.™

Haldimand

Agenda

1. Two-Factor Authentication
2. Authentication Methods for 2FA
3. Standard Operating Procedures
4. How to Identify Scams – Don't Trust Anyone!
    a. Phishing
    b. How to protect your information
5. Password Managers

What is Two-Factor Authentication

Two-factor authentication (2FA) is an identity and access management security method that requires two forms of identification to access resources and data. It requires using a second method (i.e. mobile phone, email address) to gain access.

What is Two-Factor Authentication

As you can see below, an example of the process would be:

Enter Login Information - > Mobile authentication app gives code - > enter code into login

The user enters in their username and password.

An authentication code is sent to the user's mobile device.

The user enters in their authentication code to log into the application.

What Does Two-Factor Authentication Protect us From?

- Businesses use Two-Factor Authentication to help protect their business assets.
- 2FA is important because it assists in preventing cybercriminals from stealing, destroying, or accessing your internal data records for their own use.
- 2FA will protect accounts from the majority of cyber attacks such as brute forcing attempts and email/password changes.

Authentication Methods for 2FA

Push notifications
Push two-factor authentication methods require no password. This type of 2FA sends a signal to your phone to either accept/decline access to a website/app to verify your identity.

SMS verification
SMS, or text messaging, can be used as a form of two-factor authentication when a message is sent to a trusted phone number. The user is prompted to either interact with the text or use a one-time code to verify their identity on a site or app.

Voice-based authentication
Voice authentication works in a similar way to push notifications, except that your identity is confirmed through automation. The voice will ask you to press a key or state your name to identify yourself.

Hardware tokens
Businesses can give their employees hardware tokens in the form of a key fob that produces codes every few seconds to a minute. This is one of the oldest forms of 2FA.

Standard Operating Procedures

Most businesses are aware of the importance of keeping their information safe. However, you might not often consider the importance of cybersecurity throughout the hiring process. When you're hiring remote workers especially, cybersecurity becomes an even greater priority.

- If employees will be working remotely you need to ensure that their networks are secure, especially if dealing with sensitive information. Their home network should have strong password protection.
- Discourage employees from connecting to unsecured networks or using public Wi-Fi (i.e. coffee shops, hotels, etc.).

Standard Operating Procedures

- Only give access to platforms, software, etc. that the employee will require in order to perform the duties of the job.
- Ensure that when adding them to accounts that Two-Factor Authentication is utilized.
- Doubling up on authentication and verification is essential when dealing with sensitive documents, private data, etc.

Standard Operating Procedures

Just as with onboarding, security is important when offboarding an employee

- Ensure employee no longer has access to their email account. Forward all incoming emails to another address and preserve or backup any accounts or devices. Delete employee accounts.
- Review access controls to ensure that the former employee can no longer remotely access any accounts or assets, including social media sites, software (ex. Facebook, QuickBooks, bank accounts, etc.).
- Collect all company-owned property and devices (including key cards) and update all relevant property logs (if applicable).
- Change all passwords and passcodes, and disable two-factor authentication related to the employee.

Don’t Trust Anyone

- 1 in 3 cybersecurity breaches involve a small or medium sized business
- 52% of SMBs experienced at least one cyberattack in the last year
  - 10% experienced more than 10 cyberattacks
- 40% do not have a comprehensive and up-to-date cybersecurity incident response plan

Phishing

Phishing is a type of online scam that targets consumers by sending them an e-mail or text that appears to be from a well-known source – an internet service provider, a bank, or a mortgage company, for example.

- **Don't click on links or respond to unexpected texts/calls** — Including ones asking you to fill out surveys to get free items.

Don’t Trust Anyone

- **Don’t pay a bill over the phone.** The gas company will not ask you to pay your bill over the phone using gift cards or BitCoin.

- **Don’t give personal information out online.** Answering “All About Me” online surveys that include things such as the name of your favourite teacher, your first car, etc. are social engineering tactics to gain information to answer security questions to gain access to your accounts.

7 Red Flags of Phishing

1. Urgent or threatening language
   - Pressure to respond quickly or threats of closing your account or legal action
2. Requests for sensitive information
   - Watch out for links directing you to login pages, requests to update account information or requests for financial information.
3. Anything too good to be true
   - Look out for winning a contest you never entered, prizes you have to pay to receive, or inheritances from long-lost relatives.

7 Red Flags of Phishing

4. Unexpected emails
   - Send them right to trash (ex. receipts for items you didn't buy; updates on deliveries for things you didn't order)
5. Information Mismatches
   - Watch out for incorrect sender email addresses, links that don't go to official websites, spelling or grammar errors, etc.
6. Suspicious Attachments
   - These include uncommon file types, attachments you didn't ask for, etc.
7. Unprofessional design
   - Look out for company emails with little, poor or no formatting, blurry logos, image-only emails

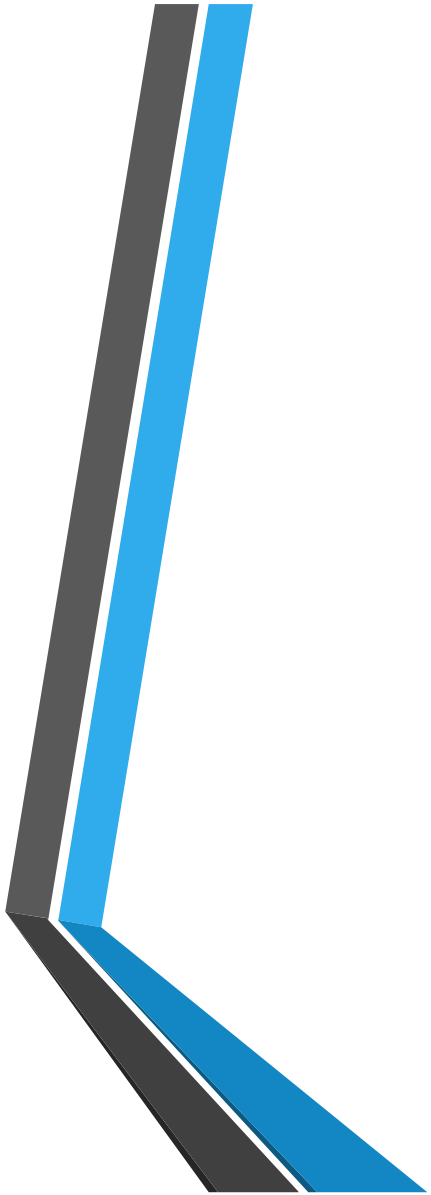
https://www.getcybersafe.gc.ca/en/resources/7-red-flags-phishing

Protect Your Information

- Verify links before you click them. Hover over the link to see if the info (sender/website address) matches what you expect.
- Avoid sending sensitive information over email or texts.
- Back up information so that you have another copy.
- Apply software updates and patches.
- Filter spam emails (unsolicited junk emails sent in bulk).

Protect Your Information

- Block IP addresses, domain names, and file types that you know to be bad.
- Call the sender to verify legitimacy (e.g. if you receive a call from your bank but don't trust it, hang up and call them).
- Reduce the amount of personal information you post online (e.g. phone numbers and extensions for employees).
- Establish protocols and procedures for your employees to internally verify suspicious communications. This should include an easy way for staff to report phishing attacks.



Questions?

Password Managers

*Please keep the password to your password manager in a safe and secure spot.

- Dashlane – https://www.dashlane.com/pricing
- 1Password – https://1password.com/business-pricing
- Keeper - https://www.keepersecurity.com/pricing/business-and-enterprise.html
- Yubikeys - https://www.yubico.com/products/

DASHLANE

- Access and manage passwords everywhere
- Zero-knowledge patented encryption which means not even Dashlane can see your passwords and passkeys
- Unlimited secure password sharing and password generation
- Dashlane continuously scans 20+ billion breach and hack records to ensure no threat goes undetected, and 2-factor authentication offers an additional layer of protection

DASHLANE Plans

Starter (for small teams & groups) **- $20.00 USD per month / billed monthly**

- 10 seats at a flat rate of $20
- Unlimited passwords & passkeys
- Secure sharing
- Dark Web insights

https://www.dashlane.com/pricing

Business (Advanced protection) - **$8 USD per seat per month / billed annually**

- Everything in the starter package plus:
- Unlimited seats
- Unlimited passwords & passkeys
- Secure sharing
- Dark Web insights
- Unlimited group collection and sharing
- Single sign-on (SSO) integration
- SCIM provisioning
- Activity Logs & advanced policies
- Enterprise deployment
- Free friends & family plan for all business users
- On-demand phone support
- VPN for Wifi protection
- Real-time phishing alerts

- Easily secure passwords, passkeys, and sensitive information.
- Monitor password health, potential breaches, and team usage from a unified insights dashboard, and take action when you need to.
- Autofill and securely share logins, two-factor codes, security questions, etc.
- Use on unlimited number of devices.

1Password Plans

Teams Starter Pack

- $24.99 CAD flat rate per month / billed monthly
- Up to 10 team members
- Built-in risk detection
- Secure password management for the whole team
- Admin controls to manage team members and share permissions
- Alerts for compromised website and vulnerable passwords
- Unrivaled 24/7 customer support
- Available on Mac, iOS, Windows, Android, Chrome OS, and Linux

https://1password.com/business-pricing

Business Plan

- 9.99 CAD per user, per month / annual billing
- Everything in the Teams Starter Pack plus:
- Scalable, secure password management trusted by over 100,000 businesses
- Admin controls to manage employees, permissions, and delegate responsibilities
- Advanced reporting for compromised employee emails and vulnerable passwords
- Customizable policies
- SSO and automated provisioning
- Free family accounts for all employees
- 24/7 dedicated business support
- Available on Mac, iOS, Windows, Android, Chrome OS, and Linux

- Secure password management for your business
- Designed for small and medium sized businesses
- Can be used on any device and/or browser
- Creates high-strength, random passwords and lets you securely share them on demand
- Each employee gets Keeper on unlimited devices for complete, company-wide protection
- When you buy Keeper Business, each team member gets a free Keeper Family Plan.
- 24/7 user support
- Autofill passwords
- Keeper utilizes proprietary zero-trust and zero-knowledge security architecture with full end-to-end encryption

Plans

Business Starter

- $2.00 USD per user/month OR $24.00 per user/annually ***Minimum of 5 users***
- Encrypted vault for every user
- Folders and subfolders
- Shared team folders
- Access from unlimited devices
- Policy engine and enforcements
- Security audit
- Activity reporting
- Team Management
- Basic two-factor authentication

Business

- $3.75 USD per user/month OR $45.00 per user/annually
- All of the features in the Business Starter plan PLUS:
- Delegated administration
- Advanced organizational structure
- Share admin

https://www.keepersecurity.com/business.html

yubico (YubiKey)

- A hardware security key that provides phishing-resistant two-factor, and multi-factor authentication
- A single YubiKey has multiple functions for securing your login to email, online services, apps, computers, and even physical spaces
- Biometric fingerprint authentication
- 1000+ integrations with most platforms

YubiKey Options

For your desktop or laptop

YubiKey Bio - FIDO Edition

$90.00 USD

Two Factor Authentication USB Security Key, Fits USB-A Ports - Protect Your Online Accounts with More Than a Password. Offers strong biometric authentication options.

For your tablet

YubiKey 5 NFC

$50.00 USD

Two Factor Authentication USB and NFC Security Key, Fits USB-A Ports and Works with Supported NFC Mobile Devices - Protect Your Online Accounts with More Than a Password.

For your mobile device

YubiKey 5Ci

$75.00 USD

YubiKey 5Ci - Two-Factor authentication Security Key for Android/Desktop/iPhone, Dual connectors for Lighting/USB-C - FIDO Certified

Please note that if you lose the physical YubiKey or any similar device, you lose access to all of your passwords

General Cybersecurity Tips

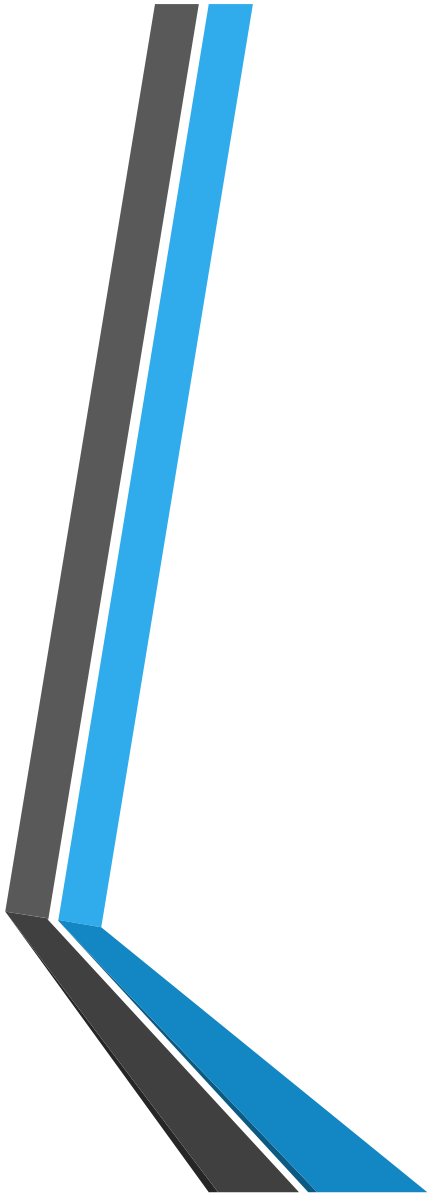
- Create strong passwords
  - Mix of upper and lower case letters, numbers, and symbols
  - Do not use the same password for multiple accounts
- Use a password manager
- Educate your team on identifying and avoiding phishing attempts
- Use two-factor-authentication
- Lock un-used devices
- Protect personal information
- Avoid unsecured/public WIFI (use a VPN if you must utilize WIFI)
- Back-up devices
- Monitor and update accounts for unauthorized access/activity
  - Ex. Ensure you have at least two people with authorized access to social media accounts so that if one person leaves, you are still able to access the page
- Keep security software updated
  - Ex. When an employee leaves, delete their authorization and change any passwords they know

Resources

- Contact: Chloe Nadrofsky (cnadrofsky@haldimandcounty.on.ca)
- Ontario Cyber Security Centre Of Excellence https://www.ontario.ca/page/cyber-security-centre-excellence
- Ontario Fraud Reporting Centre

https://www.ontario.ca/page/identify-scam-or-fraud?gclid=CjwKCAiAvoqsBhB9EiwA9XTWGbqw4R7qQ-1FohfJc5gZIYj-We8qDJCpitn8EHBpuhI5TwEGNlrjVxoChBsQAvD_BwE&gclsrc=aw.ds

- If you are interested in having a cybersecurity assessment done, please reach out and I will provide you some local businesses who offer these services.



Thank you!