



Clearbridge
Webinars

*Helping You Do Your **Best** Work*

How to Recognize a Cyberattack

**Regardless of your position,
industry, or scale of your business,
you are ALWAYS
at risk of a cyberattack.**

**60% of all targeted attacks are
aimed at small to medium-sized
businesses**

WHY?

- Less stringent security measures.
- Lack of incident response plans.
- SMBs easier to infiltrate and exploit.
- Lack means to defend/recover from attacks.



The total cost of *a single data breach* averages \$149,000 for SMBs.

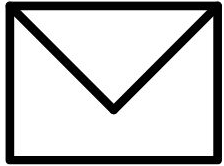
WHAT'S WORSE?

Because most SMBs have limited resources, an attack can prove ***fatal***, causing a reported **60%** of small businesses to close their doors following a cyberattack.



As we continue to say, when it comes to *cybersecurity* it's better to be PROACTIVE.

AREAS YOUR BUSINESS COULD BE COMPROMISED



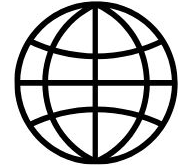
1

Email (Phishing)



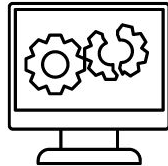
2

Files (Ransomware)



3

Network (Man-in-the-Middle)



4

System Accounts
(Social Engineering)



5

Cloud Storage
(Man-in-the-Cloud)

IN THIS NEXT PORTION

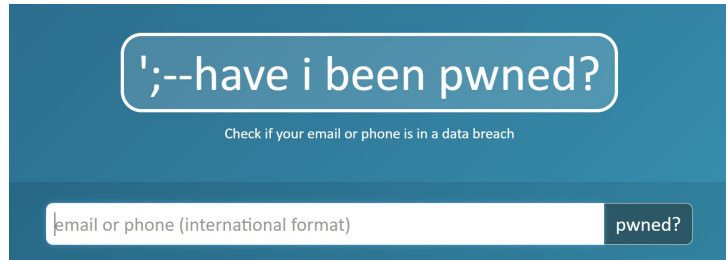
1. A proactive measure you can take
2. The signs to look for
3. What to do once you recognize the signs

***Disclaimer:* Before shutting anything down or disconnecting the network, call Clearbridge.**

1 - Your Email Account (Phishing)

PROACTIVE MEASURE

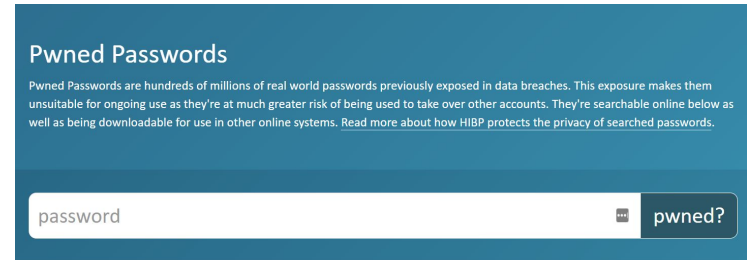
“Have I Been Pwned” is a powerful tool to check your email accounts’ safety. Enter your address and the site will check if your account has ever been part of a data breach or if your account details have been pasted online. They also have a **password tool** that determines if your password was revealed in a previous data breach.



';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?



Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

password pwned?



1 - Your Email Account (Phishing)

SIGNS TO LOOK FOR

- Your password has been changed.
- You've noticed unusual inbox activity.
- You've received password reset emails.
- Your account has been accessed from unexpected IP addresses.
- Your friends are receiving spam messages from you.

WHAT TO DO NEXT

- Use a more complex password.
- Update your account recovery information.
- Alert email contacts of suspicious activity.
- Check account forwarding and auto-replies.
- Check to see if your other accounts were affected.
- Enable multi-factor authentication (MFA).



2 - Your Files (Ransomware)

PROACTIVE MEASURE

- Employ a **data backup** and **recovery plan** for all critical information and regularly test your backups.
- Create, maintain, and exercise a **incident response plan**.
- **Be wary of emails** as they are the most vulnerable to ransomware attacks, and enable security measures like **multi-factor authentication (MFA)**.



2 - Your Files (Ransomware)

SIGNS TO LOOK FOR

- Inexplicable slowdowns on your workstation or network.
- Suspicious changes to files, names, or locations.
- Unauthorized or previously undetected extraction of data.
- Unrecognized or otherwise out of place file encryption.
- Explicit splash screen messaging indicating an attack.

WHAT TO DO NEXT

- Notify Clearbridge.
- Remain calm and collected.
- Take a photo/screenshot of the ransomware note.
- Disconnect from backups/network.
- Reset passwords.
- Inform the authorities (cyber.gc.ca/en).




3 - Your Network (MITM)

PROACTIVE MEASURE

Cyberattacks are much more likely to occur through mundane errors like a user choosing an easy-to-guess password or not **changing the default password** on something like a router.*



*We've mentioned the 2020 SolarWinds attack, where a server password was "SolarWinds123" 



3 - Your Network (MITM)

SIGNS TO LOOK FOR

- Your files and/or server have been encrypted.
- The network becomes very sluggish/slow.
- Your data usage is unusually high.
- Programs are continually crashing.
- Computers are functioning without local input.

WHAT TO DO NEXT

- Notify Clearbridge.
- Perform a security scan for malware.
- Communicate with your team and notify any affected users.
- Follow your Business Continuity Plan.
- Restore from a backup.
- Isolate the infected site (disconnect endpoints and server from the rest of the network).



4 - Your System Accounts (Social Engineering)

PROACTIVE MEASURE

It is important to have **user training** to understand how to not reveal sensitive information, and **MFA** in the event a mistake occurs.

Other accounts can inadvertently give an attacker **access to credentials or sensitive data**.



4 - Your System Accounts (Social Engineering)

SIGNS TO LOOK FOR

- Your computer speed has slowed down.
- Your security software has been disabled or compromised.
- Software or browser add-ons appear that you don't recognize.
- Additional pop-ups are happening.
- Random shutdowns and restarts are happening.
- You've lost access to your account.

WHAT TO DO NEXT

- Notify Clearbridge.
- Perform a security scan for malware.
- Communicate with your team, and keep them in the loop.
- Isolate the infected system from the network.
- Review monitoring systems to identify and understand how the threat entered.
- Enable MFA.



5 - Your Online Storage (MITC)

PROACTIVE MEASURE

Ensure you are using **multi-factor authentication** along with **encrypting cloud data** to minimize the chance of a successful attack.

One of the worst security holes — the man-in-the-cloud attack (MITC) — can compromise popular programs like Box, Dropbox, and Microsoft OneDrive. Hackers can steal the security token that gives your computer access to the cloud.



5 - Online Storage (MITC)

SIGNS TO LOOK FOR

- Your site suddenly has content that shouldn't be there.
- You cannot access your account.
- Files are missing or altered.
- You're being notified of unexpected access locations and logins.
- A large number of requests for the same file have been received.

WHAT TO DO NEXT

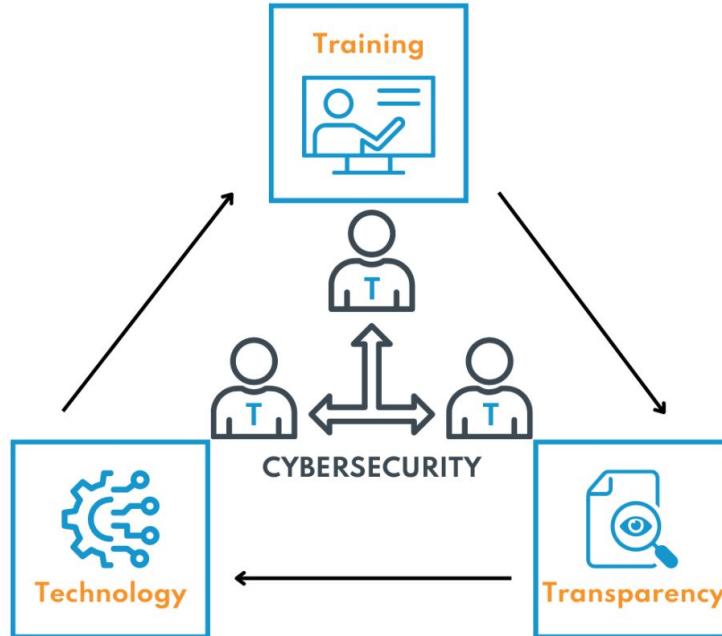
- Notify Clearbridge.
- Perform a security scan for malware.
- Communicate with your team, and keep them in the loop to determine next steps.
- Notify any affected users.
- Follow your Business Continuity Plan.
- Enable MFA.



**How can you protect *yourself*
and your *business*?**

Follow the three *Ts*!

Employees should understand and be **trained** on company policies about software use, and data ownership.



Technology should support **employees and employers** in detecting, investigating and responding to data breaches.

Employers should be **transparent** about what activities the company is monitoring on work-issued laptops.



**3 measures your business can employ
right now**

1. Go through our **10-POINT CYBERSECURITY INSPECTION CHECKLIST** to assess your cybersecurity readiness and awareness.
2. Run a **CYBERSECURITY AUDIT** to gain a clear picture of your problem areas and what issues you need to deal with.
3. Create an **INCIDENT RESPONSE PLAN** to give your team a step-by-step process to follow to manage and mitigate data breaches.



Top Tips

1. Be **SENSIBLE** - *Never* click on links, download files or open attachments in emails (or on social media) that aren't from a **known, trusted source**.
2. Be **PROACTIVE** - **Learn** as much as possible about *cybersecurity*, **get certified**, and **ask for training** at the workplace.
3. Be **VIGILANT** - *Every situation* you come across *could* be a **potential scam**. It's better to be safe than sorry. If you see something, **SAY SOMETHING**.



Q + A

support@clearbridge.ca

clearbridge.ca/resources

clearbridge.ca/lifewithclearbridge



Clearbridge
Webinars

*Helping You Do Your **Best** Work*

Thank you!