Cybersecurity: Responding to cybersecurity incidents

The Government of Alberta's Cybersecurity Services team recommends precautions and responses against cyberattacks.

We live in an increasingly digital world where cyber threats and attacks continue to increase in numbers and sophistication. The Government of Alberta's Cybersecurity Services team monitors and identifies specific types of cyber threats, recommends precautions against them and advises best practices in response to cyberattacks.

Phishing and spear phishing

Phishing attacks often come in the form of an email, text, or phone call that aims to trick the recipient into giving away information or performing an action detrimental to themselves or their organization.

Similarly, spear phishing attacks specifically target selected management, finance and other decision makers within an organization.

Phishing messages will often be spoofed to appear as though they are coming from within an organization and make unusual requests, like buying a gift card or sending a wire transfer.

What you need to do

Firstly, it is critical that you ensure that your computers and devices are protected. Please verify that your systems are protected using antimalware software such as Microsoft Defender, Trend Micro, or Norton Antivirus, and also confirm that the software is up-to-date to ensure optimal protection of your system and your data.

When you suspect that an email, text, or file you received might be a cyberattack, do not open links or attachments until you have confirmed that it is safe to do so. Hover your cursor over the name of the sender to reveal the real email of the sender. If the displayed email is different than the one identified in the "To:" field, you are likely dealing with a phishing attack.

If you are unsure about the validity of the email, search for the sender's contact information and call them to confirm whether they sent the email. If you have confirmed that the email or text is malicious, immediately report it to your organization's cybersecurity team and delete the email.

If you suspect you are receiving a phishing phone call, hang up and report the phone number to your local telephone services team. Search for an organization's contact information and call them if you would like to confirm the validity of the claims made on the call (for example, confirming whether you owe a debt or have an outstanding invoice).

Do not take any of the actions suggested or requested during a suspicious call, such as calling another phone number. These precautions apply to suspicious robocalls that use recorded messages, as well as live conversations with real people.

Ransomware

Ransomware is a form of malware (short for malicious software) that uses encryption to hold data and information hostage for ransom. Ransomware can be downloaded on a device without consent through a malicious link, email, text, or website.

What you need to do

Contact your organization's technical support as soon as you believe there is a problem.

The Government of Alberta recommends against paying ransom in response to a malware attack. Paying the ransom might seem like an easy way to regain access to data quickly, but doing so may attract more attacks with increasing ransom

demands. Paying the ransom also does not guarantee that the attacker will provide the information to decrypt your files, nor does it guarantee that the ransomware will be removed from your systems.

The best technical protection against ransomware is a good anti-malware system along with regular and tested file backups.

Ensure your staff are trained to be prepared for new and existing cybersecurity threats. Review the participation statistics of security awareness training of your organization and your specific professional area.

Disclosing the incident

Take measures to disclose the incident to potentially impacted parties as soon as possible. However, ensure that your organization has a solution in place to recover compromised information before announcing the incident publicly.

It is also critical not to disclose whether a ransom was paid as this may encourage further attacks on your organization.

Security controls

Your organization can be protected with the following security controls:

- **Physical locations**

  Protect your infrastructure by keeping the location of your organization's data centres secure. Disclosing the location of a data centre may attract physical attacks that could compromise infrastructure. Such attacks may include cutting power to the data centre, infiltrating the location, or tapping into unsecured WiFi networks.

- **Firewall and security-related software**

  Do not publicly disclose details about firewalls, anti-malware, or other security-related software. Similarly, do not disclose details of any known security or network vulnerabilities, even if they are actively being addressed. Doing so may expose gaps in your organization's cybersecurity controls that attackers may try to manipulate to gain information or access to your network.

  Take steps to ensure that staff know not to disclose details about your organization's security controls in resumes or on social media, including professional social networking sites such as LinkedIn. Attackers may be able to use this information to identify known software vulnerabilities or 'back doors' that can be used to breach your network.

- **Disaster recovery planning**

  Disaster recovery planning is an important step to ensure an organization can recovery data and services in the event of a crisis. In public messaging, refer to 'planned maintenance' rather than 'disaster recovery planning.' Attackers may target your systems while the organization is focused on recovery efforts or take advantage of weakened security set-ups to access back-up systems.

Training

Investing in training and awareness is an important first step in protecting information assets.

If your organization does not have a cybersecurity program, the Government of Alberta has developed free online courses about phishing and social engineering, malware and ransomware, and secure passwords.