RANSOMWARE – WHAT EVERYONE SHOULD KNOW

These guidelines provide information on ransomware and cyberattack prevention.

September 2023

Office of the
Saskatchewan Information
and Privacy Commissioner

Ransomware – What everyone should know

Introduction

Each year, thousands of Canadian individuals and businesses are impacted by cyber security incidents or crimes. The most common type of incident involves demands for ransomware payments, followed by threats to steal personal information or financial data. Most incidents do not include a motive.

> Ransomware is a type of malware that locks a victim's data or device and threatens to keep it locked unless the victim pays.

About half of the reported types of fraud are reported from victims of mass marketing fraud. The top reported types of fraud include phishing, extortion and personal information scams.

Types of Ransomware

There are two types of ransomware; each involves victims downloading a malicious ransomware program:

1. In the first type, the malicious program encrypts the victim's files. This makes the files unreadable or unusable. Victims are asked to pay a ransom to decrypt the files.

2. In the second type, the victim's files are transferred to the attacker. The victim must then pay a ransom to prevent their files from being shared on the open web.

How Does a Ransomware Attack Happen

Ransomware is typically spread through phishing emails. Phishing is where an attacker tricks the victim into sharing confidential information by entering it into sites that look legitimate. The intent is to obtain valid credentials or other personal information. Victims can also be targeted through text messages or by telephone.

Victims may also inadvertently download malware, which is a collective term for viruses, worms, Trojan Horses, etc. Malware is usually distributed by email as a link or file the recipient is asked to open. Once open, the malware spreads. Once it spreads, the malware can install programs that record keystrokes, block connections to files/applications or to the whole system until the user pays a ransom or can destroy components that leave a computer useless.

Can you Prevent a Ransomware Attack

The following can help prevent a ransomware attack:

- Keep your operating system and virus protection updated. Cybercriminals look for and use flaws to gain access to your devices.
- Download only the applications you require on your computer or smart device. Delete applications you no longer use.
- Install a good malware program. Avoid ones that are free or that you don't need to pay to use.
- Use two-factor authentication.
- If a link in an email is unfamiliar, do not click it. Also, a link may not be what it appears to be. Before you click on a link, hover over it to see the actual URL. Make sure the website you're being directed to is spelled correctly, and that it leads to an expected domain (such as ".com, .ca").
- Always be suspicious of emails that ask you for personal information, or that include links where you are asked to enter your credentials. For example, your bank should never instruct you to reset your password through an email link that requires you to enter login information. If in doubt, contact the company directly to ask if there is a problem with your account.
- If an email is suspicious, check the return sender's email address. For example, if you receive an email from SaskTel asking you to update your account information or to pay a bill, it is not likely that a SaskTel employee is going to send you an email from a Gmail or Hotmail account. Beware of senders you don't know, or just ignore them altogether!
- Cybercriminals usually like to make offers that seem too good to be true. These are designed to catch your attention, and may include claims that you've won a prize, etc. Remember the adage – if it's too good to be true, it probably is!
- If you're being asked to act fast, or if you're asked to do something in a limited time, it may be a tactic. For example, you may be told that your Netflix account will be suspended if you don't update your password within a specified amount

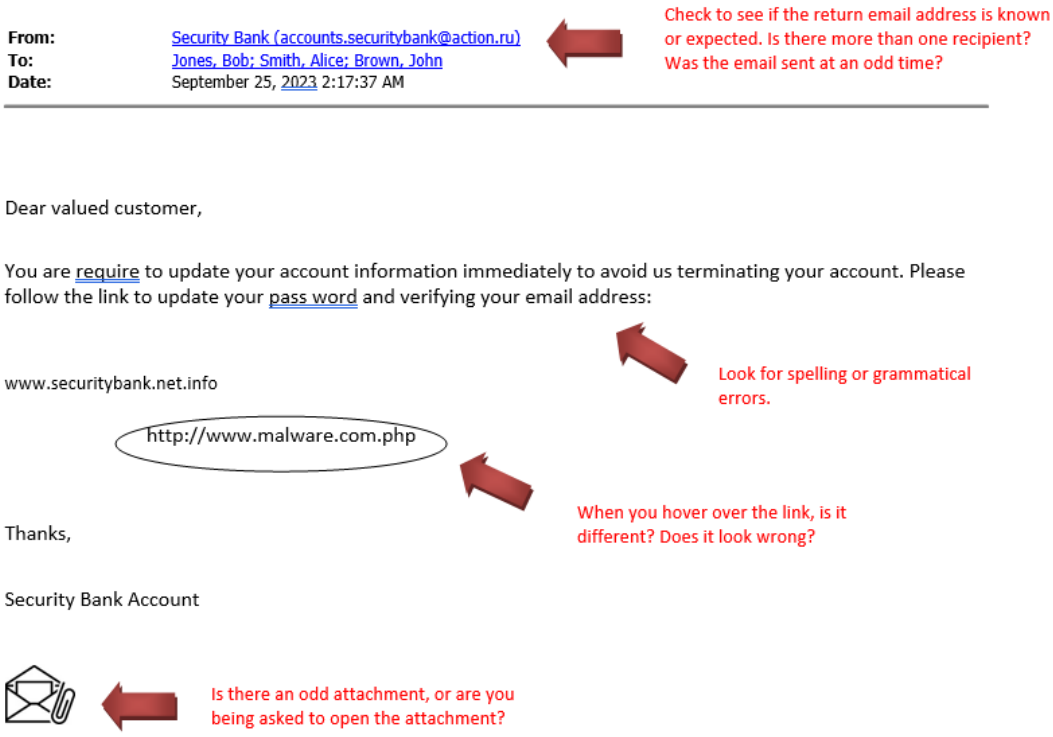
of time. A sense of urgency is designed to get you to react rather than take the time to think about what you're doing. Again, check directly with the company or service provider to determine if there is, in fact, an issue.

- Have a plan to educate employees about ransomware attacks that includes what to do if one occurs. Review this plan with employees several times a year.

Social Engineering Red Flags and Suspicious Emails

Social engineering is a way of manipulating or exploiting humans and human behaviour in a way to gain access to private information. Through social engineering, people are lured into sharing private information, downloading corrupt or infected software, visiting infected websites and sending money to criminals.

To minimize being a target, look for some of the following red flags in your emails:



How Should you Respond to a Ransomware Attack

Your response will be what you do immediately after an attack occurs and will depend on the severity of an attack. You should never wait for an attack to occur, however. Prevention is the best way to avoid a cyber security incident from occurring in the first place.

Consider the following:

- Before an incident ever occurs, have a security response in place including a security response team (e.g., IT, legal, management, etc.). Your plan should consider business continuity needs. Everyone on the team should know their role.
- Separate user accounts with administrator privileges from daily use accounts to help reduce an employee's ability to run software and to ensure they have access to only the resources necessary to do their job.
- Have strong antivirus and strong spam filters in place, use authentication technologies including two-factor technologies, implement good backup policies, segregate networks to contain future breaches, conduct routine system checks and ensure strict security measures are in place. Also consider an extended detection and response tool (XDR) as it covers a wider variety of activity, and the use of managed detection and response services where someone else monitors activity captured by the XDR.
- When an incident does occur, act quickly and seek help from experts who can help identify the cause of the infection, including which devices, applications and systems are infected. Experts can also advise on the selection or use of safe backup data, your ability to recover data, and options to recover your systems such as the reinstallation of software.
- Report the attack to the police, whose role it is to investigate. You can also contact the Canadian Anti-Fraud Centre (toll free 1-888-495-8501), which collects information on fraud and identity theft and assists the police.
- Determine if you will pay the ransom. The purpose of paying the ransom is so the attacker will decrypt your data or return it. Doing so doesn't always ensure the malware's removal. It also doesn't guarantee that the attacker will do anything, which is why experts often recommend against paying a ransom. Experts also argue that paying a ransom encourages a criminal business model, or it may lead to attackers requesting higher payments.
- Use lessons learned to develop or amend your plan to prevent future attacks.

More Information and Resources

- Canadian Centre for Cyber Security - Canadian Centre for Cyber Security
- Canadian Anti-Fraud Centre - Canadian Anti-Fraud Centre (antifraudcentre-centreantifraude.ca)
- Saskatchewan IPC webinar - https://oipc.sk.ca/media/webinars/

Contact Information

If you have any questions or concerns about these guidelines, please contact us at:

306-787-8350 | toll free 1-877-748-2298
503 – 1801 Hamilton Street | Regina SK S4P 4B4
intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC