Protecting Yourself from Cyber Scams

Safeguarding Against Cyber Scams

In the digital age, technology has opened up new opportunities and convenience, but it has also given rise to cyber threats and scams. Cyber scams are increasingly prevalent in Canada, targeting individuals and

organizations across the country. We are dedicated to the financial well-being of our members, we understand the importance of educating and empowering our community to protect themselves from cyber scams.

Types of Cyber Scams in Canada

1. Phishing Scams

Phishing scams involve deceitful attempts to obtain sensitive information such as passwords, credit card numbers, and social insurance numbers. Scammers typically impersonate legitimate entities through emails, phone calls, or text messages.

2. Identity Theft

Identity theft occurs when someone steals personal information to commit fraudulent activities, often for financial gains. This can lead to unauthorized transactions, fraudulent loans, or damage to credit scores.

3. Ransomware Attacks

Ransomware is malicious software that encrypts a victim's files or systems, demanding a ransom to restore access. These attacks can be devastating for individuals and businesses, causing financial loss and data breaches.

4. E-commerce Fraud

E-commerce fraud involves fraudulent transactions on online platforms. Scammers may use stolen credit card information to make purchases or exploit vulnerabilities in online payment systems.

5. Tech Support Scams

Scammers pose as tech support agents, claiming issues with your computer or software. They trick individuals into granting remote access or paying for unnecessary services, potentially compromising personal data.

6. Romance Scams

Romance scams prey on emotional connections, with scammers building relationships online and then requesting money for various reasons. Canadians have fallen victim to these heartless schemes, resulting in financial losses and emotional distress.

Protecting Yourself from Cyber Scams

1. Educate Yourself and Others

Stay informed about the latest scams and educate your family, friends, and colleagues. Awareness is the first line of defense against cyber threats.

2. Use Strong and Unique Passwords

Create complex passwords for each online account, using a mix of letters, numbers, and special characters. Avoid using easily guessable information like birthdays or names.

3. Enable Multi-Factor Authentication (MFA)

Implement MFA wherever possible, adding an extra layer of security by requiring at least two forms of identification before granting access.

4. Verify Requests for Personal Information

Be cautious when asked for personal or financial details via email, phone, or messages. Verify the request through a trusted and official communication method before providing any information.

5. Regularly Update and Patch Software

Keep all software, including operating systems, browsers, and antivirus programs, up to date with the latest security patches and updates to minimize vulnerabilities.

6. Use Reputable Antivirus and Anti-Malware Software

Install and regularly update reputable antivirus and anti-malware software to detect and remove malicious programs that could compromise your devices.

7. Be Cautious with Email Links and Attachments

Avoid clicking on suspicious links or downloading attachments from unknown sources. Hover over links to see the actual URL before clicking.

8. Secure Your Wi-Fi Network

Protect your home Wi-Fi with a strong, unique password and encryption. Change default router passwords and use WPA3 encryption for enhanced security.

9. Monitor Your Financial Accounts Regularly

Regularly review your bank and credit card statements for any unauthorized transactions. Report any suspicious activities to your financial institution immediately.

10. Exercise Caution on Social Media

Be mindful of the information you share on social media platforms. Avoid posting sensitive personal information that could be used by scammers.

11. Backup Your Data

Regularly back up important files and documents to a secure, external location. In the event of a ransomware attack, you can restore your data without paying the ransom.

12. Stay Informed About Current Scams

Frequently check trusted sources like the Canadian Anti-Fraud Centre (CAFC) and the Better Business Bureau for updates on recent scams and fraud prevention tips.

Cyber scams continue to evolve, becoming more sophisticated and pervasive. By staying informed and adopting proactive measures, we can reduce the risk of falling victim to these scams. At GVC Credit Union, we are committed to promoting financial security and empowering our members to safeguard their lives. Stay vigilant, stay safe, and together, we can create a more secure digital landscape.