6 SIMPLE WAYS TO

Help Keep Your Business Cyber Safe

With so many employees working remotely and cyber threats on the rise, it's essential that businesses know how to protect themselves from fraud. Share this guide with your employees to help them stay safe from cybercrime.

PHISHING, SMISHING & VISHING

Scammers send you a text or email pretending to be from the government, a bank, or another business.

They can direct you to a website that looks legitimate – but isn't. They may ask you to update or verify your password, account or other confidential information.

BUSINESS EMAIL COMPROMISE

Criminals send you an email or phone call pretending to be a senior executive of your company, a long-time vendor or someone else you trust.

They want you to send a wire transfer or they request confidential information.

MALWARE

Criminals send you a link or attachment in an email, text, or pop-up window.

Malicious software, or *malware* can get installed when you click a link or open an attachment. Criminals can use malware to steal information and find out your passwords, security questions or token values.

1

THINK BEFORE YOU CLICK

Be suspicious of unknown links that you were not expecting.

Hover over the link to check its destination. Be extra suspicious if the link contains a lot of unusual characters, hyphens, numbers, spelling mistakes, symbols or links that lead you to web pages with unusual forms, especially those that require you to enter sensitive information. Before entering credit card information, ensure the URL starts with HTTPS and validate that is a trusted site. HTTP sites are not secure, and any information entered on them could be compromised.

2

DOUBLE CHECK EMAIL

Ensure the sender's email reflects the actual email address of your vendor, colleague.

Hover over the email with your cursor to see the actual email address. You can also hover over any links to view the full URL and check where the link would actually take you.

3

BE AWARE OF SCAMS

Be aware of common phishing scams, malware and fraud schemes so you can avoid them.

Instruct your employees to use caution with unexpected links, attachments, unusual payment requests or requests for confidential information. Visit the Canadian Anti-Fraud Centre to view the latest scams. Always remember, Scotiabank will never ask for confidential information through text message or email.

4

PASSWORD HYGIENE

Implement strong passwords that are easy for you to remember yet hard for others to guess.

Make your passwords as long as you can and include numbers, letters and symbols. Memorize passwords instead of writing them down on paper. That paper can be seen, copied or stolen.

5

PROTECT DEVICES WHEN OUT OF YOUR HOME OR OFFICE

Remember that smartphones, tablets and laptops are easy to steal.

Always keep an eye on your devices and be mindful of others nearby. Also, restrict the use of public Wi-Fi for work because these networks are less secure.

6

PLAN AHEAD WHEN EMPLOYEES LEAVE

When an employee leaves the organization, make sure their physical and system access is removed promptly.

Hackers can quickly exploit an unused account without anyone noticing.

Want to learn more?

STAY SAFE FROM SCAMS
Learn more about email and phone fraud

GET CYBER SAFE
Find out about cyber safety at home and work

CANADIAN ANTI-FRAUD CENTRE
Stay on top of the latest fraud so you can avoid them

CYBER SAFE GUIDE FOR SMALL & MEDIUM BUSINESSES
Get more tips and advice to help keep your business safe

Scotiabank®