Understanding Cybersecurity & Payment Fraud

Worried about the safety of your banking transactions and information? You're not alone. Rapid advances in technology and the growing sophistication of fraud attempts make every organization a target for electronic payments fraud. But even with high-quality cybersecurity systems, you should take steps to protect yourself and your information.

62% **of U.S. organizations** report being exposed to actual or attempted fraud.[1]

30% **of companies in 2014** that were subject to payment fraud suffered a financial loss from the attack.[1]

$445 billion **Estimated annual cost** of cybercrime and economic espionage to the world economy.[2]

Tip: Don't be phishing bait

Phishing emails are designed to fool you into thinking they're coming from a legitimate site, like your bank. But the real intent is to gather your personal information or get you to download malicious software.

450,000 phishing attacks were identified globally in 2013.[3]

5.9 Billion financial losses attributed to worldwide phishing attacks in 2013.[3]

Over the last 12 months phishing attacks have grown from **19.9 million to 37.3 million, an increase of 87%**.[2]

Do: Regularly update your anti-virus and anti-malware software.

Do: Download IBM®* Trusteer Rapport®*[5], a free software download available to BMO® clients. It's designed to help protect against financial malware threats and works with existing firewall and antivirus software to provide an additional layer of security. To download, visit: **trusteer.com/landing-page/bmo**

Don't: Click on links or download information from emails or the Internet unless you know the source to be legitimate.

Tip: Watch what personal information you share

23% of recipients now open phishing messages and **11%** click on attachments.[4]

50% open emails and click on phishing links within the first hour.[4]

Do: Make sure that any personal or financial information you share is only with secure sites. If in doubt, type in the URL you know to be accurate.

Do: Beware of requests for credit card information. Never give card information unless you can validate that the request is legitimate.

Do: Keep your debit or corporate card and PIN safe. Do not write your PIN down or make it visible to others at payment terminals.

Don't: Give out your personal identity credentials or any financial information such as account information, usernames, passwords, PINs, security token and token password.

Tip: Create payment processes that limit exposure to fraud

In **60%** of cases, attackers are able to compromise an organization within minutes.[4]

Do: Separate duties for payment initiation and approval to ensure dual validation.

Do: Establish funds transfer limits that do not exceed your company's maximum anticipated needs.

Do: Put spending controls and blocking in place for specific cardholders and transaction categories.

Don't: Release a payment without verifying the source of the funds transfer requests. Obtain verbal confirmation from the requestor in-person or using a phone number you know to be genuine.

Let's connect

For more information, please contact your BMO Representative or visit:

bmo.com/security
bmo.tps@bmo.com

BMO Bank of Montreal
We're here to help.™

[1] 2015 AFP Payments Fraud and Control Survey, Association for Financial Professionals. [2] Economic Impact of Cybercrime 11, Center for Strategic and International Studies June 2014. [3] RSA Fraud Report for 2014. [4] 2015 Data Breach Investigations Report by Verizon Enterprise Solutions. [5] Downloading and use of the software is governed by the terms of the Trusteer Rapport license agreement. By downloading and installing Trusteer Rapport software, you agree to Trusteer Rapport's terms and conditions. Bank of Montreal is not responsible for, nor do we guarantee, this software, or other products or services of IBM. Bank of Montreal is not responsible for any difficulties, consequences, costs, claims, damages or losses arising in any way whatsoever in connection with the downloading or use of the software. Any problems, questions or concerns regarding Trusteer Rapport should be directed to IBM.

01/16-0268