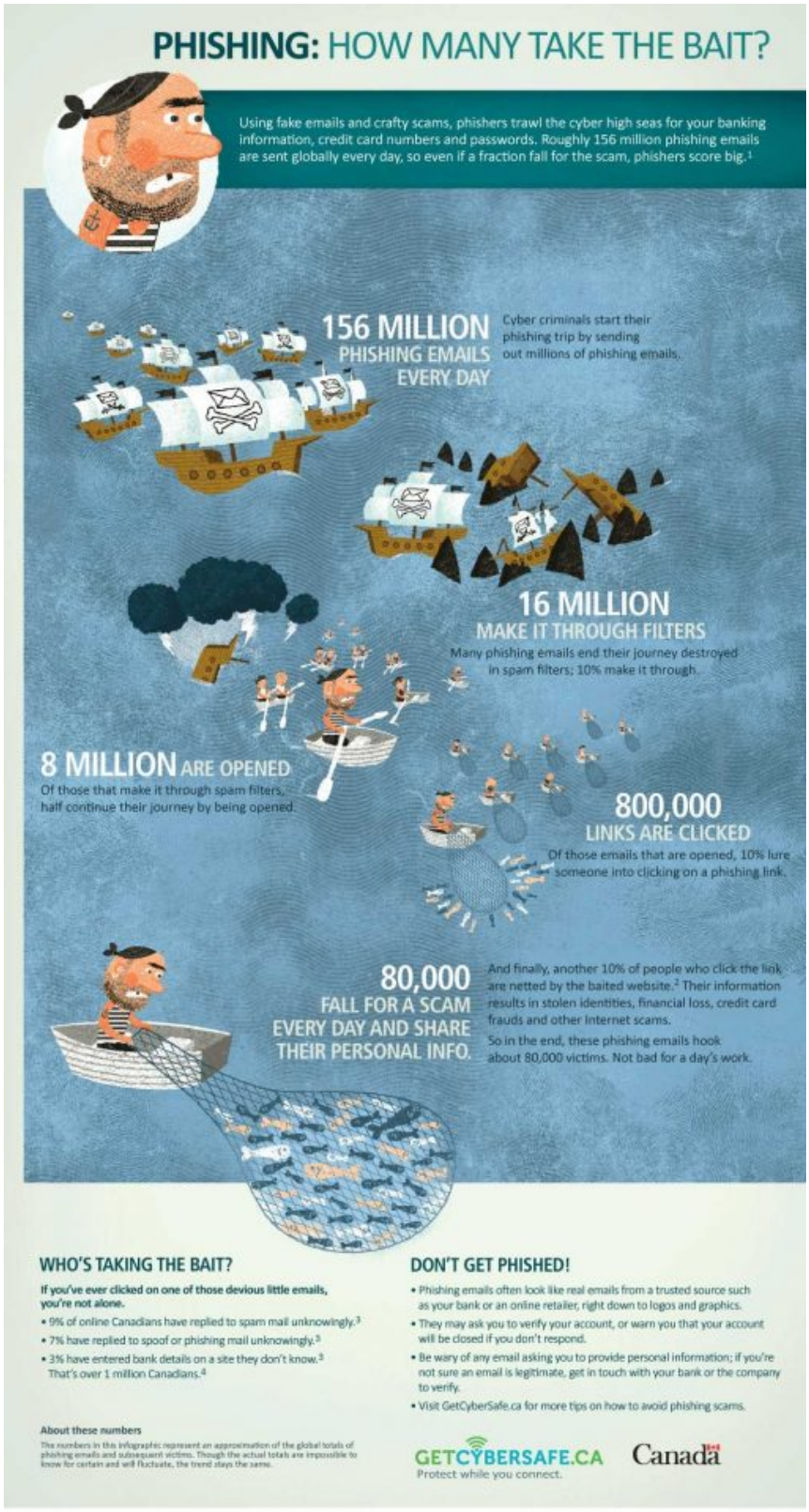
Finances and the Other F Word: Fraud and Your Money

Fraud is no joke. You've no doubt seen news stories about money transfer scams: emails promising you $7 million dollars if you transfer money from Nigeria.

Have you ever wondered how people fall for fraud scams? Well, it's a lot easier than you may think, and it can have you using a few other choice F words if it happens to you. In our busy, automated world, it is easy to accidentally click on a pop-up ad, open a random spam or phishing message, or download an infected file. You may think you're replying to an online shopping order confirmation, but with a simple click, you may download malware that accesses your personal data or unwittingly share information with a scammer.

Financial fraud was the topic of a recent Greater Niagara Chamber of Commerce Lunch n' Learn I spoke at and hearing those F words probably turned a few stomachs. At this event myself, and Detective Sergeant Paul Spiridi of the NRP Central Fraud Unit, helped educate businesses and consumers about a few types of fraud to watch out for and what to do if the F bomb happens to you.



[1] Symantec Security Technology and Response Group, August 2012
[2] Cyveillance, "The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks," 2009
[3] EKOS Research Associates, "Baseline, Online Probability Survey of Internet Users Regarding Cyber Security," 2011
[4] Based on the Statistics Canada estimate of Canada's population of about 34,880,000, July 2012

Watch Out

Fraud scams are constantly changing – so how do you know what to watch out for? Educate yourself. The The Little Black Book of Scams: Your Guide to Protection Against Fraud by the Competition Bureau of Canada explains a few types of fraud, including:

1. Money transfer requests (e.g., asking for wire transfers or e-transfers of funds)
2. Internet scams:

- malware (installs software on your computer to record/access your personal information, etc.),
- phishing (tricking you into handing over personal and banking details),
- spam emails (sent with the hope that you click on a link that will install malware/ransomware to gain access to your device), and
- online auction and internet shopping scams (may lead to purchasing items that are never delivered or the recording of personal data, etc.)

3. Mobile phone scams (someone gains access to your personal data and open a mobile phone account in your name which results in large phone bills, stolen phones to gain access to your personal information or your contact information, text scams that try to make you click on a link to install malware on your system, etc.)

Typically, internet and mobile scams use high tech tools that look and sound real to get you to share your financial information or your money.

According to Detective Sergeant Spiridi, Niagara residents fall victim to all of these types of fraud. In addition, debit and credit card fraud continue to be big problems, as well as elder abuse-related fraud and various forms of identity theft and fraud. He notes that phishing scams can also be particularly problematic. Keep your eyes peeled for our upcoming identity theft blog which will go into this in greater detail.

For example, several Niagara residents have fallen victim to a recent phishing scam that tricks people into believing they owe the Canada Revenue Agency thousands of dollars. The scammers pretend to be a company that works with tax payers to pay outstanding bills to keep victims from being arrested. Victims are told to purchase iTunes gift cards for the amount of the outstanding bill and to give the gift card numbers to the scammers, who will transfer the funds to the CRA.

It may sound like a rather obvious scam, but Detective Sergeant Spiridi notes that high-pressure tactics and personal circumstances lead many people to fall for it. Sometimes victims are tipped off by cashiers when they try to purchase the gift cards. Other times they lose their money to the scammers.

Stay Safe

Ultimately, it is your responsibility to protect yourself from financial fraud in daily life. Although your financial institution may safeguard the transmission of data and its backend, it cannot protect your devices. In addition, as Detective Sergeant Spiridi notes, given the nature of online scams, it is very difficult to track down perpetrators. Your credit card from Welland may be used to make purchases in Tennessee, but it may have been accessed during a security breach by a company you shared your credit card information with 2 years ago. With such international implications, it is impossible for Niagara police to track down who made purchases in your name and thus often impossible to get your money back.

So what can you do to stay safe? To protect yourself Detective Sergeant Spiridi and myself recommend a few tips:

1. Keep your operating and anti-virus systems up-to-date on ALL your devices – yes that means your phones, tablets, and computers.
2. Use caution online. Check for “https” or the lock logo in the address bar before entering your personal information. Avoid downloading from less-than-reputable sites. Go directly to websites instead of clicking on email or mobile links. Scammers can copy brand logos and create very realistic messages and fake sites to trick you into sharing your personal information.
3. Check your financial statements every month. Ensure no unauthorized transactions have occurred and report them immediately if they have.
4. Review your credit report annually. Look for unauthorized companies checking your credit, purchases that you did not make, and things like credit cards, lines of credit, etc. that you did not apply for. Often people are unaware of identity theft until they hear from a collections agency – so don’t wait – proactively check your credit. Equifax and TransUnion are two trusted sources.
5. Educate yourself about fraud and how to protect yourself from the Canadian Anti-Fraud Centre and Consumer Protection Ontario.

Check out this blog to learn more about how to stay safe from fraud.

Dropping the F Bomb

What do you do if you are the victim of fraud? Depending on the type of fraud, you may report it differently. If you have lost money, Detective Sergeant Spiridi acknowledges that your options may be limited. Here are few things you can do:

- If an unauthorized transaction happens in your account, report it to your financial institution *immediately* for investigation and resolution (the sooner you report the problem, the better chance you have of stopping transactions and saving your money)

- Report fraud *immediately* to other appropriate authorities when you lose money and recognize you might not get it back
- Learn more about fraud and how to protect yourself from the Canadian Anti-Fraud Centre and Consumer Protection Ontario

The F bomb can have a huge effect on your life. Educate yourself about how to stay safe and take steps to protect yourself. Also, remember that if something seems too good to be true, it probably is. Getting rich quick may seem like a possibility, but it is usually only the scammers that get rich off your misfortune.