Protect Yourself From Online Fraud

A Division of Thomas Edison Electric

Information taken from the RCMP Website

http://www.rcmp-grc.gc.ca/

Inside this issue:

A Division of Thomas Edison Electric

Online Scams and Fraud

Recognize It

What is Phishing?

Phishing is a general term for e-mails, text messages and websites fabricated and sent by criminals and designed to look like they come from well-known and trusted businesses, financial institutions and government agencies in an attempt to collect personal, financial and sensitive information. It's also known as brand spoofing.

FACTS

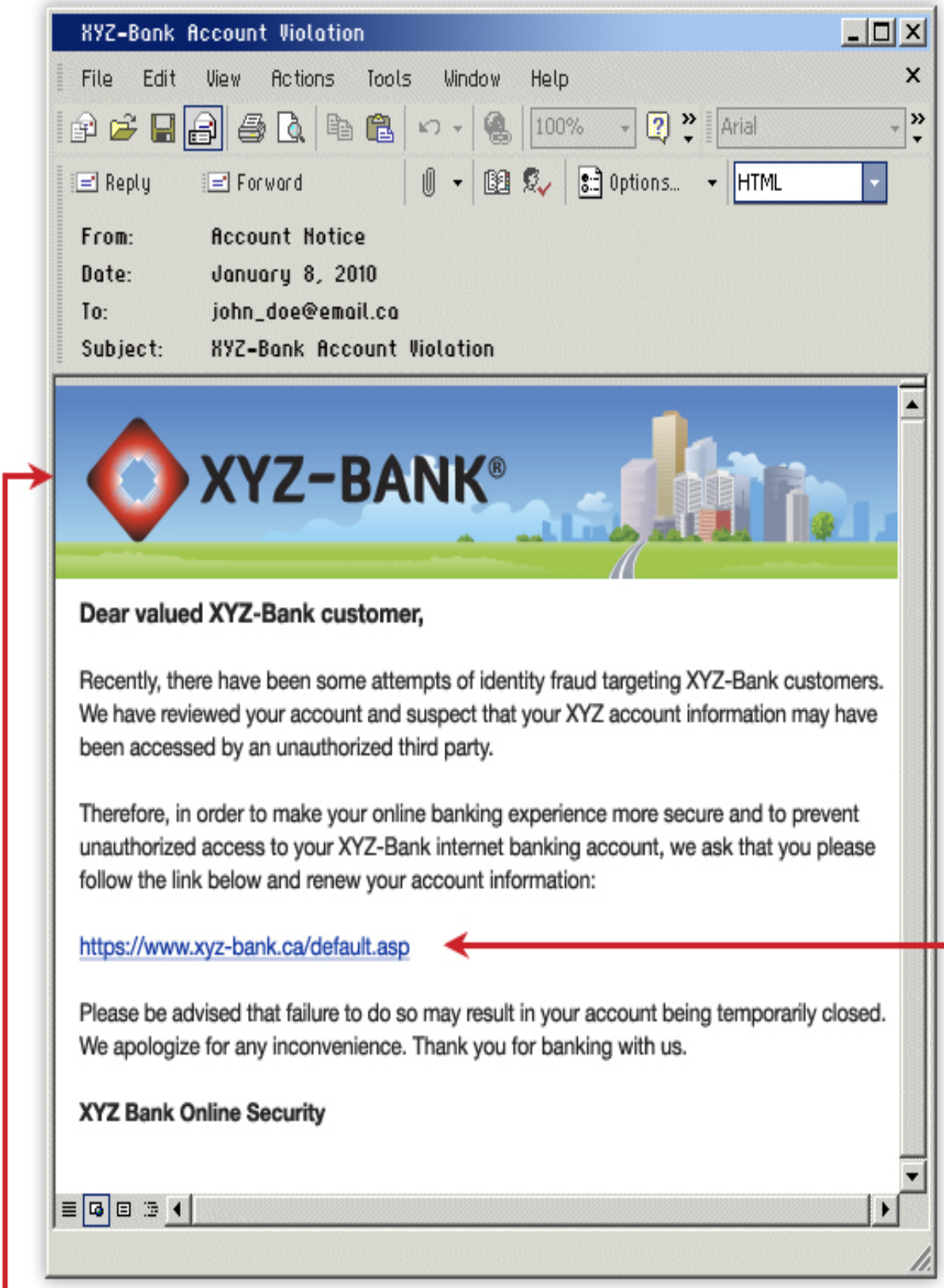
Characteristics

- The content of a phishing e-mail or text message is intended to trigger a quick reaction from you. It can use upsetting or exciting information, demand an urgent response or employe a false pre-tense or statement. Phishing messages are normally not personalized.
- Typically, phishing messages will ask you to "update", "validate", or "confirm" your account information or face dire consequences. They might even ask you to make a phone call.
- Often, the message or website includes official-looking logos and other identifying information taken directly from legitimate websites. Government, financial institutions and online payment services are common targets of brand spoofing.

Catch Phrases

- *E-mail Money Transfer Alert: Please verify this payment information below…*
- *It has come to our attention that your online banking profile needs to be updated as part of our continuous efforts to protect your account and reduce instances of fraud…*
- *Dear Online Account Holder, Access To Your Account Is Currently Unavailable…*
- *Important Service Announcement from…, You have 1 unread Security Message!*
- *We regret to inform you that we had to lock your bank account access. Call (telephone number) to restore your bank account.*

Example Of A Phishing E-mail on Page 4



Graphic from bank's actual web site which looks identical.

http://203.144.234.138/us/index.html

In some cases, the offending site can modify your browser address bar to make it look legitimate, including the web address of the real site and a secure "https://" prefix.

Information sought: Social insurance numbers, full name, date of birth, full address, mother's maiden name, username and password of online services, driver's license number, personal identification numbers (PIN), credit card information (numbers, expiry dates and the last three digits printed on the signature panel) and bank account numbers.

What your information could be used for: Phishing criminals can access your financial accounts, open new bank accounts, transfer bank balances, apply for loans, credit cards and other goods/ services, make purchases, access your personal email account, hide criminal activities, receive government benefits or obtain a passport.

Report it

If you receive one of these suspicious e-mails:

Report it to the Canadian Anti-Fraud Centre or the institution that it appears to be from.

If you received one of these suspicious e-mails and you unwittingly provided personal information or financial information, follow these steps:

- **Step 1** - Contact your bank/financial institution or credit card company
- **Step 2** - Contact your credit bureau and have fraud alerts placed on your credit reports:
- Equifax CanadaToll free: 1-800-465-7166
- TransUnion CanadaToll free: 1-877-525-3823

Step 3 - Contact your local police

Step 4 - Always report phishing. If you have responded to one of these suspicious e-mails, report it to the Canadian Anti-Fraud Centre

Stop it

How to prevent

- Be suspicious of any e-mail or text message containing urgent requests for personal or financial information (financial institutions and credit card companies normally will not use e-mail to confirm an existing client's information).
- Contact the organization by using a telephone number from a credible source such as a phone book or a bill.
- Never e-mail personal or financial information.
- Avoid embedded links in an e-mail claiming to bring you to a secure site.
- Get in the habit of looking at a website's address line and verify if it displays something different from the address mentioned in the email.
- Regularly update your computer protection with anti-virus software, spyware filters, e-mail filters and firewall programs.
- A number of legitimate companies and financial institutions that have been targeted by phishing schemes have published contact information for reporting possible phishing e-mails as well as online notices about how their customers can recognize and protect themselves from phishing.
- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

Identity Theft and Identity Fraud

Recognize it

What is Identity Theft?

Identity theft refers to the preparatory stage of acquiring and collecting someone else's personal information for criminal purposes. As of January 8, 2010, Senate Bill S-4 became law, making it illegal to possess another person's identity information for criminal purposes.

What is Identity Fraud?

Identity fraud is the actual deceptive use of the identity information of another person (living or dead) in connection with various frauds (including for example personating another person and the misuse of debit card or credit card data).

Facts

- Identity theft techniques can range from unsophisticated, such as dumpster diving and mail theft, to more elaborate schemes.
- Technology, mainly the Internet, facilitates more elaborate schemes, such as skimming, phishing, and hacking as criminals gather profiles of potential victims. Computer spywares and viruses, designed to help thieves acquire personal information, are an emerging trend.
- Victims of identity theft or fraud can experience financial loss and difficulty obtaining credit or restoring their "good name".
- In 2009, the CACF received identity fraud reports from 11,095 Canadian victims, totaling a loss of more than 10 million dollars. This represents an increase of more than 1 million dollars of what was reported in 2008. Payment card fraud was the most commonly reported incident, and yet, many instances of identity theft and fraud go unreported.

Information sought

Identity thieves are looking for the following information:

- full name
- date of birth
- Social Insurance Numbers
- full address
- mother's maiden name
- username and password for online services
- driver's license number
- personal identification numbers (PIN)
- credit card information (numbers, expiry dates and the last three digits printed on the signature panel)
- bank account numbers
- signature
- passport number

The new legislation on identity theft provides a complete list of identity documents.

The new section 402.1 of the *Criminal Code* lists the definition and examples of identity information.

What your information could be used for

Criminals can use your stolen or reproduced personal or financial information to:

- access your bank accounts
- open new bank accounts
- transfer bank balances
- apply for loans, credit cards and other goods and services
- make purchases
- hide their criminal activities
- obtain passports or receive government benefits

  Using identity theft to facilitate organized criminal and terrorist activities also appears to be a growing trend.

How can you find out if your identity was stolen

The best way to find out is to monitor your hard copy or on-line financial accounts frequently and to check your credit report regularly for any unusual activities. If you receive calls from collection agencies about unfamiliar accounts, or if you applied for credit and were unexpectedly turned down, you should investigate further.

Report it

If you suspect or know that you are a victim of identity theft or fraud, or if you **unwittingly provided personal information or financial information:**

- **Step 1** - Contact your local police force and file a report.
- **Step 2** - Contact your bank/financial institution and credit card company
    - **Step 3** - Contact the two national credit bureaus and place a fraud alert on your credit reports.
- Equifax CanadaToll free: 1-800-465-7166
- TransUnion CanadaToll free: 1-877-525-3823

Step 4 - Always report identity theft and fraud. Contact the Canadian Anti-Fraud Centre

Stop it

Prevention is the best way to deal with this crime:

- Identity theft can occur over the Internet or telephone, or via fax or regular mail. Therefore, be particularly wary of unsolicited e-mails, telephone calls or mail attempting to extract personal or financial information from you.
- Ask yourself if you really need all of the identity documents you carry in your wallet or purse. Remove any you don't need and keep them in a secure place instead.
- Periodically check your credit reports, bank and credit card statements and report any irregularities promptly to the relevant financial institution and to the credit bureaus.
- During transactions, it's safer to swipe your cards yourself than it is to allow a cashier to do it for you. If you must hand over your card, never lose sight of it.
- Always shield your personal identification number when using an ATM or a PIN pad.

Stop it Continued

- Memorize all personal identification numbers for payment cards and telephone calling cards. Never write them on the cards.

- Familiarize yourself with billing cycles for your credit and debit cards.

- Trash bins are a goldmine for identity thieves. Make sure you shred personal and financial documents before putting them in the garbage.

- When you change your address, make sure you notify the post office and all relevant financial institutions (your bank and credit card companies).

On-line shopping fraud: from a buyer or seller's point of view

Recognize it

What is on-line shopping fraud?

These days, Canadians can buy or sell almost anything over the Internet. Unfortunately, criminals can use the anonymity of the internet to rip off unsuspecting buyers and sellers.

For example, scammers may sell a product – often at a very cheap price – just so they can steal your payment card or personal information. They may also take your money and send you a worthless item, or sometimes, nothing at all.

What is on-line auction fraud?

On-line auction sites are virtual flea markets that present new or used items for sale that you can bid on. On-line auction scams include such frauds as the misrepresentation of an item, non-delivery of goods and services, as well as non-payment for goods delivered.

On-line auctions can be rigged by scammers. If you are selling a product, the scammer can enter a low bid followed by a very high bid under another name. Just before the auction closes, the scammer withdraws the high bid and the low bid wins. If you are buying a product, the scammer can boost the price using dummy bidders.

Important information

- Most on-line auction websites have an on-line learning guide and security tips on proper on-line payment methods and precautions. These payment methods are very secure and may minimize the risk of fraud while offering purchase protection.

- The sellers are the focus of most Internet auction fraud complaints.

- If you buy or sell on-line, you should also be aware of cheque overpayment scams. In this type of scam, you are sent a cheque for something you have sold, but the cheque is made out for more than the agreed amount. The scammer hopes you will refund the extra money before noticing that his cheque has bounced.

Report it

If you are a victim of on-line shopping fraud:

- **Step 1** — Contact the police service of jurisdiction in your area.
- **Step 2** — Report the fraud to the Canadian Anti-Fraud Centre by going to their website or by calling 1-888-495-8501.
- **Step 3** — You should also report the crime to the on-line shopping website you dealt with.

Stop it

- Deal with companies or individuals that you know by reputation or experience. If you are not familiar with the company, do some research. Reputable on-line merchants will post plenty of information about themselves, their location, their phone and fax numbers and details like their membership in organizations such as the Better Business Bureau.
- Look for a privacy policy. Be sure you are comfortable with how the company collects, protects and uses your personal information before you submit any details. Responsible marketers have an opt-out policy, which allows you to choose whether your information is shared with third parties.
- Do not be lured into using payment methods other than the options recommended by the Internet auction site. Do not pay by sending cash, money transfers or money orders.
- Consider using a company that provides an escrow service (reliable third-party). Escrow agents will hold the buyer's payment until they have received notification that the goods or services have been delivered. The escrow service then delivers the payment to the seller or provider. Research the credibility of the escrow service approved by the on-line auction service provider. Beware of criminals who create fraudulent escrow sites by mimicking legitimate sites or creating entirely fictitious sites to get money from trusting victims.
- Shop only from your home computer. It's much safer than shopping at a terminal in an internet café or library.

Stop it Continued

- Verify secure connections. When shopping on-line, do not enter any financial information on a site if you see a broken key or an open padlock symbol in your Internet browser. This means the transaction is not secure and could be intercepted by a third party. When the key is complete or the padlock is locked, your browser is indicating a secure transaction.

- Consider using a credit card with a low credit limit or a single use payment card.

- Monitor your bank and credit card statements on-line. Electronic statements allow you to review your purchases and payments as they happen rather than waiting until the end of the month to review your paper statement.

- Never give out your social insurance number, date of birth or driver's license number to a seller.

- Before you bid, learn as much as you can about how the on-line auction works, your obligations as a buyer, and the seller's obligations.

- Always remember, if an offer sounds suspicious or too good to be true, it probably is.

Protecting Your Information Online

Everyone has an online profile these days, but sometimes we aren't aware of how to make sure that what we post online stays private. Remember – what goes online is pretty much there for life. Here are some tips that can help you protect your online reputation:

- **Are your security settings set to "Friends Only?**" Websites like Facebook update their security settings often (and usually without warning), so check your settings at least once a week. Make sure the settings are as private as you're comfortable with – you don't want strangers liking your pictures do you?!

- **Is there any swearing on your profile?** Posting things online can seem harmless, but they can actually affect your future. For example, if there's swearing all over your profile, your future employers could find it – and they probably wouldn't be impressed with your language!

- **If a police officer looked at your profile, would you be worried about what they could find?** Are there are any pictures of you online doing anything illegal (like underage drinking or doing drugs)? If you wouldn't want a police officer to see it then leave it offline, because anything online is fair game to be used by police officers. Or better yet, just make sure you aren't doing anything the police would have to deal with.

- **Have you met each of your contacts?** You may add complete strangers to your profile to make new friends, or to make your friend count higher. Whatever the reason, allowing strangers to see all of your personal information is just creepy. If you wouldn't share personal details with a stranger on the street, then why let them access it online?

- **Does the message look suspicious?** What scammers, hackers and phishers are able to pull off these days is endless. Bottom line is, if it looks suspicious, don't click it. If you get a message from a friend or stranger and it looks kind of sketchy, ask the sender personally if the message came from them before you open it.

- **Can strangers find you?** Sharing details like your first name and gender are okay, and so is sharing your general location (e.g. "Canada" or "Ottawa"). But sharing things like your phone number, home address or even what school you go to makes it easy for anyone to find you. If you don't want to get spammed, end up a victim of identity theft or let Joe Shmoe know where you live, then keep personal information like your phone number and email address off your profile.