Could this happen to you?

Would you take the bait on a phishing scam?

"Phishing" is one of the most common scams that cyber criminals use because it can produce spectacular results with very little effort or expense on the part of the hacker. Phishing involves the use of an email, text message or phone call that appears to come from a trusted source or institution, vendor or company, but is actually from a third-party impostor. Phishing messages are intended to trick you into giving cyber criminals your information by asking you to update or confirm personal or online account information. Personal information and identity theft and/or payment scams are the motives behind most phishing scams. Thousands are phished – criminals only need one or two dupes to make it pay off.

Cyber criminals do their best to make phishing messages look official and legitimate. They will mimic real communications from the company or entity they are supposedly from by using the same layout, fonts, wording, message footers and copyright notices, etc. as official messages. They will often include corporate logos and even one or more links to the alleged sender's real website.

To make it more likely you will fall for the scam, phishing messages commonly involve urgent scenarios. They may suggest that you must reset your password because your account has been compromised by hackers or they may request that you login to your account to review an invoice or deal with an outstanding payment. Another common phishing scam is a call from someone claiming to be from Microsoft who will tell you your computer is infected and that you must go to a special website to download an update that will fix the problem. Phishing scams can also be a request to complete a survey or to give information to collect a prize you have won. They can also be requests for money supposedly from someone you know (see the "stuck in London" example on the next page).

Many phishing messages will include a link or attachment that you are asked to click so you can update your information. After doing so, the webpage or attachment you will see (which will also have text and logos to make it look official) will prompt you to enter your name, account number, password and other personal information – thereby giving it to cyber criminals.

To make matters worse, clicking on links or attachments in phishing messages often causes malware to be downloaded to your computer as well.

Could it happen to you? Would you fall for a phishing scam?

As you consider these questions, see the next page for some sample phishing messages.

How to spot phishing messages

Phishing scams work because some people are gullible. If you get a phishing message from a bank and you don't have an account there, you aren't likely to fall for the scam. However, if you have an account at that bank, the message may look legitimate to you and you are more likely to fall for the scam. Here are some clues that can help you recognize a phishing message:

- The link you are asked to visit is different from the company's usual website URL (see the next paragraph).
- The main part of the sender's email address is not the same as the company's usual email address.
- Bad spelling and poor grammar.
- Nonsensical or rambling content.
- The promise of receiving money or another big prize.
- Anyone asking for money – even if you know them (see the "stuck in London" message on the next page).

QUICK FIX

Checking the link you are asked to go to is one of the best ways to confirm that a message is a phishing scam. Place your mouse over the link you are asked to go to (but don't click on it!) and look at the taskbar in your browser window (usually at the lower left). It will show you the URL of the link. It should start with the proper characters in the proper website (e.g., lawpro.ca) and not a URL that appears unrelated (e.g., http://12.67.876/aed/1234/bnklogin). An unrelated URL virtually guarantees it is a phishing scam. Watch for small differences: "lawpro.com.tv" seems close, but is different!

QUICK FIX

Never respond to "phishing" requests for personal information in the mail, over the phone or online. Most importantly – this is probably the most common way that personal information is stolen – never ever reply to unsolicited or suspicious emails, instant messages or web pages asking for your personal information (e.g., usernames, passwords, SIN number, bank account numbers, PINs, credit card numbers, mother's birth name or birthday), even if they appear to be from a known or trusted person or business. Legitimate businesses should never send you an email message asking to send your username, password or other information to them in an email message. If in doubt, call the company yourself using a phone number from a trusted source. Don't use the number in the email – it could be fake too! ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LawPRO.

Sample phishing scam messages

A message pretending to be from RBC re hacked account

From : RBC (service@rbcanada.com)
Subject : Account Alert !

Actions for current recipient :

Dear your email address

Your password was entered incorrectly more than 5 times.

Because of that , our security team had to suspend your accounts and all the funds inside.

Your account access and the hold on your funds will be released as soon as you verify your information.

Review Your Account Activity

We are sorry for this inconvenience but this is a security measure which we must apply to ensure your account safety.

If you have already confirmed your information then please disregard this message

Thanks for choosing Royal Bank of Canada

The RBC Security Team

Copyright © 1999 – 2013 RBC. All rights reserved.

A message pretending to be from a debtor re payment request

From : Ann Tara <office@schaechle.com, herira7@aol.com>
Subject : Invoice Payment Confirmation

Actions for current recipient :

Hello

My name is Ann Tara , i was asked by my boss to send you the payment been made Earlier today.

Kindly see the attached payment slip for confirmation. Thus acknowledge the receipt of payment been made.

Thanks

Attachments
PaymentCopy.zip, 192330 bytes

A message pretending to be from Wells Fargo

From : alerts@notify.wellsfargo.com
Subject : Wells Fargo: Changes to Your Membership Checking Account

Actions for current recipient :

Important changes coming to your Membership Checking Account

There are important changes coming to your Membership Checking account that will take effect November 7, 2013.

Please sign on to view a secure message about these changes.

Thank you. We appreciate your business.

Sincerely,
Wells Fargo Online Customer Service
wellsfargo.com | Fraud Information Center
Wells Fargo Bank, N.A. Member FDIC.

Please do not reply to this automated email.

A message pretending to be from PayPal re account correction

From : PayPay l Inc.account@ppl.ca
Subject : Restore your account.

Dear PayPal Customer,

During our regularly scheduled account maintenance and verification procedure we have detected a slight error in your Paypal account.

This might be due to the following reasons:

1. A recent change in your personal information (ie. change of address, email address)

2. An inability to accurately verify your selected option of payment due to an internal error within our systems.

Please fill in all the details that are required to complete this verification process. To do this we have attached a form to this email. Please download the form and follow the instructions on your screen.

Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporary suspend your account.

Sincerely,
PayPal

Please do not reply to this email because we are not monitoring this inbox.

Copyright © 2013 PayPal, Inc. All rights reserved.

Attachments:

Restore.your.account.html, 11036 bytes

A message pretending to be from a friend via Google Drive

Google Drive. Keep everything. Share anything

Please check the document I uploaded for you using Google docs.

CLICK HERE just sign in with your email to view the document it's very important.

Thank You.

—

Someone you know
Street Address
Toronto, Ontario
Postal code

A message addressed to you from someone you know "stuck in London" asking for money

[Note: If you are getting this message, it likely means the person that it is from has had their email account hacked, likely by a phishing scam they fell for.]

Subject: Please help me

Hello,

I'm sorry for this odd request because it might get to you too urgent but it's due to the situation of things right now.

I'm stuck in London, England right now, I came down here for a short vacation then i was robbed, worse of it is that bags, cash and cards and my cell phone were stolen at GUN POINT, it's such a crazy experience for me, I need help flying back home, the authorities are not being 100% supportive but the good thing is i still have my passport and return ticket but currently having troubles paying off the hotel bills and also getting a cab to take me to the airport.

Please i need you to loan me some money, will refund you as soon as i'm back home, i promise.All i need is ($900 USD) but dont know how much you would be able to spare..we will be waiting to hear back from you on how you can get the fund to me please

Thank You