

Examples of Common Phishing Scams: How to Spot and Avoid Them

November 28, 2016



205-828 Harbourside Drive
North Vancouver, BC V7P 3R9

Phone 604 980 2700
www.netcetera.ca

What is Phishing?

Phishing is a social engineering strategy used to obtain sensitive information such as usernames, passwords, credit card details, intellectual property, business and personal data (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.





FROM:

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address **from a suspicious domain?** (like micorsoft-support.com)
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.



TO:

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



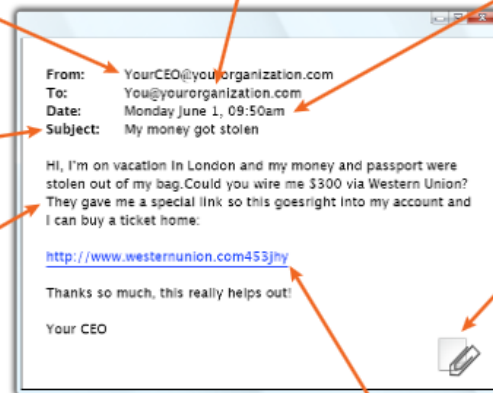
DATE:

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT:

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested?**



ATTACHMENTS:

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me these types of attachment(s).)
- I see an attachment with a **possibly dangerous file type**. The only file type that is **always safe to click on** is a **.TXT** file.



CONTENT:

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence**, or to **gain something of value?**
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors?**
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical?**
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?



HYPERLINKS:

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters - "r" & "n".





Sat 11/26/2016 8:10 PM

Important <no-reply@mail.ndu.edu.ng>

Important Notice

To Steve Weeks

If there are problems with how this message is displayed, click here to view it in a web browser.

This is an example of a phishing e-mail I received today. At first glance it looks relatively legitimate, but when you look a little closer you start to see the telltale signs of a phishing scam.

Look at the sender's e-mail address. Does it look like it came from PayPal?

Notice the poor grammar in the text. Would PayPay have poor grammar in their e-mails?

Would PayPal send e-mails with spelling mistakes? (e.g. memorise instead of memorize)

Stay updated on your account.

steve@netcetera.ca



Unusual Activity On Your Account
steve@netcetera.ca

Someone has login to your account. If not yours, please login and check your account in link below.

Solve Now

Because unusual activity in your account, now your account has been limited, login to your account now and review your identity on link above

Why checkout with PayPal?

- + Earn Reward Points
Grow your credit card rewards as you shop with PayPal. Simply add and link a credit card to shop.
- + Buyer Protection
If an eligible item does not show up, or turns out to be significantly different, we will help sort things out
- + Easier and faster
No more mindless numbers to memorise. Shop with just an email and password.
- + Refunded returns
If you need to send eligible items back, we will refund up to USD15 off your shipping fees.

[Account](#) [Help](#) [Fees](#) [Security](#) [Apps](#) [Shop](#) [Language Preference](#)

How do I know this is not a spoof email?
Spoof or "phishing" emails tend to have generic greetings such as "Dear PayPal member". Emails from us will always address you by your given email.

This email was sent to steve@netcetera.ca, because your email preferences are set to receive the PayPal Periodical newsletter and Product Updates. To unsubscribe, please click [here](#).

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Copyright © 2016 PayPal. All rights reserved.

More poor grammar.

They want you to click on this link. Doing so will redirect you to a fake PayPal login page. Entering your credentials will give them what they want - full access to your PayPal account.

Several poorly worded sentences.

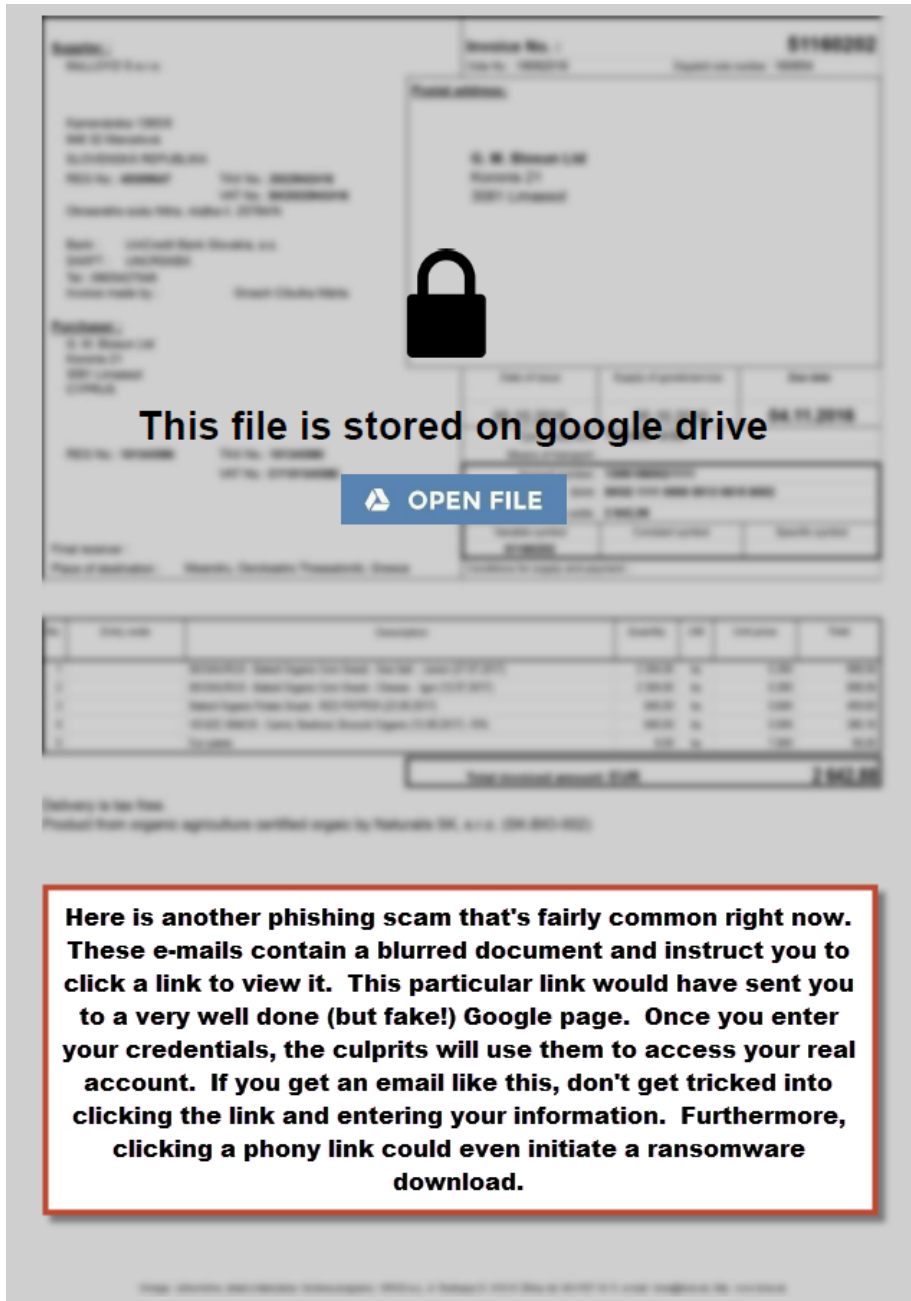
Did you notice that they make a point of calling you by name? This is done to try and convince you that they're legitimate.



205-828 Harbourside Drive
North Vancouver, BC V7P 3R9

Phone 604 980 2700
www.netcetera.ca

This is great information but what about my home computers?



This file is stored on google drive

OPEN FILE

Here is another phishing scam that's fairly common right now. These e-mails contain a blurred document and instruct you to click a link to view it. This particular link would have sent you to a very well done (but fake!) Google page. Once you enter your credentials, the culprits will use them to access your real account. If you get an email like this, don't get tricked into clicking the link and entering your information. Furthermore, clicking a phony link could even initiate a ransomware download.

All the same rules for business apply at home as well. On most home networks, the weaknesses we see on a regular basis are described below:

Outdated and unpatched software. One of the easiest things to do is ensure your PC or MAC is running the latest versions of its operating system and application software. Once you're up to date, set up automatic updates to ensure you stay current going forward.

Many people either do not have antivirus software, use outdated software or they use any software they can find for free. Whether you're using a PC or a MAC, we recommend using the same Sophos software products you trust at work. You can download the Sophos software for home use, for free, from the following site:

For a Windows PC or a MAC: www.sophos.com/home

The other common mistake we see is people failing to back up their home PC or Mac. We have seen firsthand the panic, anger and sense of loss people feel when important documents and treasured family photos are lost forever. To avoid this, you can purchase a small removable hard drive and backup your device locally, regardless of whether you run a Mac or PC.

On a MAC, use the built in Time Machine software. On a PC, use the software that comes included with a removable hard drive. In addition to the local backup, you can sign up for iCloud (on a MAC) and OneDrive (on a PC), both of which will capture off site copies of all your data. These are just a few of the many backup options available to you.

Finally, follow all the recommendations we have included for business use (see below) to keep home devices safe and secure



Steps you can take to help keep your business network and your data safe

- Make sure your operating systems and all applications are up to date and patched
- Install a properly configured commercial grade firewall with up to date firmware and licensing
- Make sure all of your servers and endpoints are running a properly configured, commercial grade antivirus solution, with up to date definition files
- Whatever antivirus solution you're running, consider adding on Sophos InterceptX, which is currently the most effective ransomware and zero day virus protection available. Read our blog about InterceptX here: www.netcetera.ca/about-us/blog/
- Have a backup and disaster recover solution in place and test it regularly. We recommend Datto: www.datto.com
- Use only legitimate software and be wary of freeware
- Do not login with admin level credentials for day to day work
- Educate and encourage everyone to adopt a philosophy where security is everyone's responsibility
- Pause and think before you click, look for clues that indicate this e-mail may not be legitimate (see above)
- Be aware that even well-known legitimate websites can be compromised, especially the advertising links. This is commonly referred to as "malvertising"
- Use strong passwords and change them regularly (Minimum 8 characters, including lower case, upper case, numbers and special characters)
- Consider adding a sandboxing service to detonate (test run) unknown attachments and links outside of your internal network
- Never plug in or attach unknown external devices (memory sticks, removable drives, etc.) to your computer
- Tighten up the security settings in your browser's (Safari, Edge, Internet Explorer, Firefox, Chrome, etc.) security options
- Avoid using file sharing sites (Box, Google Drive, DropBox, etc.) unless absolutely necessary. If you do use them, make sure they are backed up and the data has been encrypted prior to putting it out there
- Do not enable macros unless you absolutely have to, and only if you trust the source or confirm with the sender before enabling
- Educate yourself as much as possible and stay current with the latest threats making the rounds
- Trust your gut, it's usually right. If in doubt, delete! Don't open or click
- Doing any on-line shopping? Never use your work e-mail and passwords for this purpose. You put your company at risk if you do.
- If you have any concerns talk to us about a security audit

We've provided you with a number of ways to protect yourself and your business, and there are many more that could be added to this list. Even adding just a few of these tips into your regular policies and procedures could prevent you from being a target. The more strategies you utilize, the more you reduce your risk of falling victim to a cybercriminal.

Have a great and safe holiday season.
Netcetera...



205-828 Harbourside Drive
North Vancouver, BC V7P 3R9

Phone 604 980 2700
www.netcetera.ca