alpha numérique

SUMMARY

To click or not to click: recognizing and protecting oneself from phishing

What is Phishing?

According to the *Canadian Centre for Cyber Security*, phishing is defined as follows: “Phishing is a general term for emails, 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.”

What are the different types of online scams?

EMAILS

Scammers send targeted emails to fool their victims and steal their private information.

SOCIAL MEDIA

Scammers use social media to spread false information and thus lure their victims.

WEBSITES

Scammers create fake websites that seem legitimate in which they copy official logos.

Phishing by email: what is spam?

Spam is unsolicited email messages sent to a large group of people (advertisement, gift or request for money). The message is designed to conceal the true email address/identity of the sender and often contains harmful links.

If you replied to a suspicious email, provided personal information or lost money, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501.

7 warning signals of a phishing message

1. PRESSURE OR THREATENING LANGUAGE

Real emergency messages are rarely sent by email.

2. SENSITIVE INFORMATION ASKED

Trustworthy organizations or individuals rarely ask to provide this type of information by email.

3. TOO GOOD TO BE TRUE

It is uncommon to win the lottery without participating or to receive an inheritance from a relative that we have never heard of!

4. UNEXPECTED EMAILS

Receiving receipts or follow-ups about articles that were never ordered is rather surprising.

5. Dubious INFORMATION

Following your instinct and looking for signs might help you identify phishing. Here are some thoughts that might help:

- Is the sender's email address correct?
- Do the links lead you to an official page?
- Are there spelling or grammar mistakes that a legitimate organization knows how to avoid?

6. SUSPICIOUS ATTACHMENTS

Being cautious is important, especially if the names or type of files that accompany an email are unusual or have spelling mistakes.

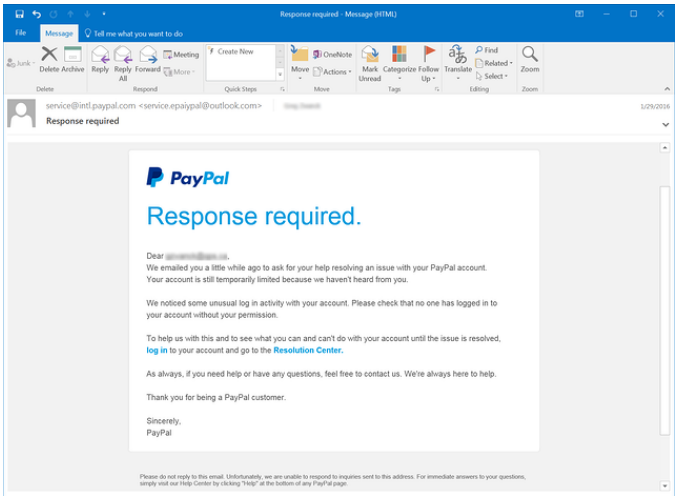
7. AMATEUR GRAPHIC DESIGN

Cybercriminals rarely hire professional graphic designers. Pay attention to blurred or inaccurate logos as well as page layouts that are dubious.

The four steps of a phishing email

1. You will receive a message that seems to come from a relative or an institution.
2. You are asked to take urgent action by clicking on a link or an attachment.
3. You provide personal information in a message, or you fill-out an online form on a website that seems reliable.
4. The fraudster uses this information without your consent.

Here are two phishing examples that warn you about an emergency or a problem:



I clicked on a link or I opened an attachment from a fraudulent email.What can I do?

If you did not provide your confidential information:

- Change your password for that website immediately.
- Apply the same procedure for all your confidential accesses.

If you did provide your confidential information:

- Contact your local police
- Your banking institutions
- Notify credit agencies such as Équifax (1 800 465-7166 or 514 493-2314) and TransUnion (1 877 713-3393 or 514 335-0374). They will add a note to your file to warn credit grantors that you might been a victim of fraudulent activity.

Recognizing a fraudulent post on social networks

- The person who published the post does not seem legitimate.
- You are encouraged to click on a dubious link that does not lead to an official website.
- The post may contain several spelling and grammar mistakes.
- A threatening tone is generally used.
- An urgent context is often established so that you may act quickly.
- Some parts are often written in another language.
- The comments written under the post seem fake, even invented.

Websites and security: How to recognize a fraudulent website?

- The address is different from the one that is registered
- Spelling and grammar mistakes
- The logos that are used are different from the official logos
- Fonts and font colours are uneven
- The page layout of the form to complete is simplistic
- Use of general expressions to give a sense of credibility

HTTPS: why is this important?

To meet the ever-increasing security requirements on the Web and to make things difficult to hackers, Google took the decision, in 2017, to penalize non-secure sites that use an HTTP protocol, that is to say, the vast majority! Furthermore, Google announced recently that in July 2018, the domains that did not have the HTTPS authentication yet, will appear on Google Chrome's browser, as "non-secure."

Keep learning on alphanumerique.ca!