VUB Informatieveiligheid en Privacy

How To – Recognize Vhishing, Phishing en Smishing

Verantwoordelijke:
Chief Information Security Officer

Contact(en):
ciso@vub.be

Laatste update:
30 maart 2020

I. Overzicht

A “How To …” document provides information and/or hints and tips about a specific Information Security and Privacy (ISP) topic. It does not contain a mandatory standard/guideline. Rather, it provides information about how a standard/guideline can be applied.

It is a ‘living’ document whose quality depends partly on the feedback from its readers/users. The cover page gives the contact email address to which feedback can be sent.

A “How To” document does not follow a formal consultation and approval process.

II. Herken Vhishing, Phishing en Smishing

II.1. How do I recognise Phishing, Vishing and Smishing?

Cybercriminals are increasingly trying to steal sensitive data from you via fake emails, websites and messages. To reduce their chances of succeeding, we’ve got a few tips to help you recognise this sort of message. Because the best security against cyberattacks begins with you!

Via email (‘phishing’), phone (‘voice phishing’, or ‘vishing’) or SMS (‘smishing’), criminals hope to gain sensitive information such as passwords, usernames or bank details. A common tactic is to misuse information that at first glance appears to be trustworthy and useful to you. But how do you recognise a suspicious message?

II.1.1. The sender

Ask yourself questions about the sender of a suspicious email or phone call: Do you know them? Have you had contact with them before? Have you actually received a reminder to pay them? Do you know this ‘friend in need’? Is their email address correct? Watch out: even a legitimate email address is no guarantee of trustworthiness.

II.1.2. The recipient(s)

Look at the other recipients of the email, and the people in CC. If the email has been sent to an unusually large group of people with nothing in common, or who you don’t know, then be careful. Is the message in your spam or junk folder? Be extra careful if so.

II.1.3. The delivery date

Have you received an email that should normally have been sent during office hours at a strange time, such as 3.00 in the morning? Then be extra alert.

II.1.4. The subject

Check if the subject of the email is connected with the content of the message, and whether it claims to be a reply to an email that you didn’t send yourself (look out for ‘RE:’ at the beginning of the subject line).

II.1.5. The content of the email

See if the content of the message makes sense. An official agency will never ask for your password, bank details or personal information via email. Spelling and grammatical errors are also often an indicator of a suspicious email. Messages with general and vague forms of address or that use your email address as a salutation are also not to be trusted.

II.1.6. The (hyper)links

Hyperlinks can be very dangerous. Often the sender will ask you to open an attachment, but clicking on just one suspicious link can endanger an entire organisation. You can best check a suspicious link by hovering the mouse over it **without** clicking: the complete address will be displayed. If it leads to another website, then it's dangerous. Is the domain name really that of the organisation?

So, in the link www.safeonweb.be/tips, the domain is 'safeonweb.be', and in the link www.safeonweb.tips.be/safeonweb, 'tips.be' is the domain and you will be taken to another website.

II.1.7. The attachments

The biggest risk, and the most commonly used by hackers, is a corrupted attachment. If you're not expecting an attachment, don't open it! Only files that end in '.txt' can be safely said to contain no virus. All other documents, such as Excel or PowerPoint files, can be infected!

II.1.8. Smishing

SMS is increasingly used as to send messages containing fake links with the aim of scamming people. This form of phishing even has a name: smishing, or SMS-phishing. The same applies here: never click on the link. If you have clicked, do not fill in any fields and stop any further interaction. If, during a conversation with the scammer they bring up payment, contact your bank and report it to the police.

II.2. What if?

If you have given out your VUB username and/or password, immediately change your password and notify the helpdesk at helpdesk@vub.be.

If you've given out your bank details, contact your bank immediately and block your card via CardStop (https://cardstop.be/en/home.html).

.1. What if you're unsure?

Never click on a link or attachment. If you think it is an attempt to scam you, delete the message from your inbox by clicking 'shift' and 'delete' at the same time and contact the sender if you know them. If the message is from a friend's address, let them know via phone, SMS or social media that their account has been hacked. On some social networks, you can mark messages as 'fake'. In organisations or companies, go to their site and check if the apparently 'urgent' offer exists. If you don't find anything, you can call to notify them.

You can forward fake messages, including SMS, to helpdesk@vub.be.

.2. Office 365

To make it easier for Office 365 users to report phishing, a button has been added to Outlook (mobile and desktop versions) and to webmail:

Select the email and click on this button. The suspicious message will then be automatically sent to the helpdesk, who will contact you if more information is needed.

.3. Be extra vigilant for coronavirus messages!

More hackers are taking advantage of the consequences of the coronavirus, especially since during these uncertain times we have been taken out of our comfort zones and are in need of extra information and social contact. Hackers are therefore using subjects that engage us emotionally or professionally in order to smuggle their malware past us.

.3.1. *Look out for illegal versions of the interactive map by Johns Hopkins University*

Cybersecurity experts are warning about a program that allows you to follow the evolution of the virus on a map of the world. A dashboard of coronavirus infections and deaths created by Johns Hopkins University has been misused by malicious websites to install viruses that can detect and steal passwords. The installation only works if JavaScript is enabled.

Only use the official link: https://coronavirus.jhu.edu/map.html

.3.2. *Covid-19 Tracker App contains ransomware*

The Android COVID19 Tracker App, which allows you to monitor cases of Covid-19, has been infected with the ransomware CovidLock. This denies the user access to their phone and forces them to change the password. Users then see a screen that tells them they must pay $100 in Bitcoin within 48 hours. If you do not comply, the hackers threaten to delete all the data from your device and publish all your contacts, photos, videos and social media accounts online.

Keep yourself and VUB safe!

You can find the latest information at ivp.vub.be