HORNETSECURITY

INFOPAPER:
DETECT PHISHING AND ACT CORRECTLY

Content

WHAT IS PHISHING?

Phishing is a form of fraud where the victim is sent a fake email, which is often not recognized as such, at first. The attacker uses **phishing to trick the recipient into disclosing sensitive data.** This includes personal data and passwords.

The economic damage of cyberattacks, which begin with targeted phishing attacks, are estimated by the Federal Office for Information Security to be in the double-digit millions annually. For users, there are **various risks** that can vary depending on the motive of the attacker. For example, the stolen data is used for account looting or further hacker attacks on companies. The most **common method used for phishing is the mass mailing of emails with fake-content.**

But targeted attacks are also becoming increasingly popular: In spear phishing, attackers research their victims in advance. They pretend to know their victims personally, trying to gain their trust and thus obtain valuable data.

How do I recognize a phishing email?

Recognizing a professionally designed phishing email is often not easy for the every day person - but it is not impossible either. The **following points were developed together with the experts from the Hornetsecurity Security Lab** and help to identify phishing emails on the basis of different characteristics.

Sender

Often cyber-criminals write **in the name of online-shops, such as Amazon and eBay, or from online-banking platforms, like PayPal.** The detailed view of the email address can provide information about the true origin of the message. If it is not plausible or contains misspelled characters or cryptic numbers, this is a warning sign.

An example: noreply@amzon.com instead of noreply@amazon.com. Meanwhile sender-addresses completely fake, which is why the email should be checked for other phishing characteristics. The Security Lab also recommends **checking the email header** to get detailed information about the message.

Information containing the origin of the email, which can be found in the **received lines.** These document all servers and hosts through which the email passes. As a rule, you can view the detailed view of the header in the email program under „View" or under „Options".

Receiver

In addition to the sender, the recipient can also provide information about the trustworthiness of an email. For example, if a user has logged into PayPal with a Google Mail account, but has received an email from PayPal to a GMX address, it may be phishing. This is of course is only an indicator of if the user is also using multiple email addresses.

Salutation

In large-scale phishing campaigns, cyber-criminals send their fake messages to hundreds, sometimes thousands of recipients. Often, the **correct form of address for the recipient falls by the wayside.** Especially when a supposed contractual partner suddenly no longer knows the name of the recipient and uses **general salutations** instead, caution is advised.

Layout, spelling and grammar

Cyber-criminals from abroad often use spellchecker programs to write their fake emails. Depending on the complexity of the topics and sentences, this often results in more or less serious errors. Punctuation also plays a role in the recognition of a phishing email: In addition to **misplaced commas and hyphens, foreign characters can also appear in a fake email.** The experts from the Hornetsecurity Security Lab also recommend paying attention to the **quality of the layout** of the email. Often, graphical errors indicate a phishing attack.

Psychological pressure

The **exertion of pressure** plays a crucial role in the composition of phishing emails. Cyber-criminals exert pressure on the recipient of an email in order to put „critical thinking" out of action. Often, the **recipient is threatened** with severe consequences and penalties for inaction, causing them to act quickly and rashly.

Even supposed detailed knowledge should make the victim believe the sender. An example of this is the „sextortion" trick. The cybercriminal pretends to be in possession of video footage that is hacked webcam was recorded and shows the recipient during sexual acts or similar.

In order to prove that the cybercriminal really hacked the victim's computer, sometimes even **correct passwords are listed**, although these are from old data leaks. Cyber-criminals blackmail their victims with these recordings and ask them to make a payment, usually in the form of Bitcoins or other crypto currencies.

Links, phishing pages and attachments

Cyber-criminals often try to get the recipient to open a URL. The **unsuspecting user is directed to a fake website where he or she enters personal data** and unknowingly shares it with the hacker. In order to identify damaged or fake links, it is important to check, among other things, whether the link matches the sender who sent it.

Links that contain numbers in addition to the name of the respective institution should be given special attention. Some links hide behind a URL that appears trustworthy. To see the actual destination of the link, users can hover over the URL without clicking on it to see the display hover text. The **hover text shows the entire target URL.** Cyber-criminals often use subdomains and an extension of the link with additional characters to hide the domain to which the user is actually directed. It is often difficult to tell whether a website is genuine or fake.

The abbreviation https:// was once considered a sign of a secure connection, but this only means that the website operator has acquired an SSL certificate. **Cyber-criminals can also acquire this certificate** for their website - so the abbreviation does not necessarily mean that the all-clear has been given. An indication of a phishing website could, however, be the request of a transaction number without a previous transaction having been made.

Caution is also advised, if for example, after logging on to online banking, **data that is actually known, such as**

Links, phishing pages and attachments

name and address or the IBAN, is to be entered. If one is not sure whether the URL given in the email really leads to the correct website, users should call up the website address known to them directly in the browser and enter the account data there. Email attachments can also carry risks. Hackers often use malicious attachments, especially when attacking companies. They send **alleged invoice account statements or business letters in formats such as *.xls, *.doc or *.pdf.** These contain Trojans, which log data entries and pass the information on to the cyber-criminal. Before the opening of an attachment, the recipient of the message should always check the sender, e.g. with the detailed view of the email header (Chapter: Sender) or by phone.

Request for confidential data

Users need to be particularly vigilant when dealing with **emails originating from companies in the financial sector.** If an email asks for personal information or secret numbers and passwords, this is an indication of phishing. Serious banks usually ask for sensitive data, such as PIN numbers, in writing in letter form.

SECURITY MEASURES

For protection against phishing attacks, users can take some security precautions that can protect accounts in case of an emergency. Even after a user has fallen victim to an attack, the right action afterwards can not only serve to limit damage, but also protect others from the perfidious attacks.

Password security

The **responsible use of passwords** can limit further consequential damage in the case of a successful phishing attack. Users should use a unique password for each online account. If a hacker gets hold of log-in data that is used several times, in the **worst case all accounts are at risk.**

Two-Factor Authentication

With two-factor authentication, the user is able to create an additional security level. A common **two-factor system** is the sending of a confirmation code to another device. In this way, the sensitive data of the user account is secure - even if a hacker has already captured the access data for it.

Awareness

It is important to be aware of the tactics and scams of fraudsters - this will help you to detect them more quickly or identify similar tactics. In addition to technical protection, it is essential to **become aware of the perfidious scams.**

The creativity of cyber-criminals is limitless: they often pick up on current events and use emotionally charged topics to lend credibility to their messages.

Bank customers in particular fall victim to scams like this. Cyber-criminals sent fake emails on behalf of PayPal, which referred to the DSGVO, which recently came into force at that time.

There are **internet sites, such as the consumer advice centre, where current phishing methods are listed.** A glance at the list can often reveal whether you have been the victim of a fraudulent email.

Emergency measures

If cyber-criminals have managed to get hold of a user's access data via a phishing email, the **user can still protect himself.** If it is still possible, the user should log in to the affected account as soon as possible to **change the password.**

In addition, it should be checked whether changes have already been made to the account or even transactions, such as a bank transfer, have been made. If this is the case, it is recommended to **block the affected account as soon as possible.**

Report phishing attacks

Phishing emails and phishing websites can be reported to the sender from whom the email is purported to originate. Information to the **phishing radar of the consumer advice centre** is also useful. The fake emails are listed here and can thus be found by other users. Employees can report potential phishing attacks at the company-internal IT security officer, so that the IT security companies can react accordingly.

When using an email security service, any **anomalies that indicate a phishing attack should be reported** to the responsible provider.

Checklist

- ☑ **Check sender:** Do I know the sender? Are cryptic numbers or letters in the sender address? Which IP address is displayed in the header?
- ☑ **Receiver:** When using different email accounts, make sure you use the correct address: Have I registered with PayPal using my GMX or Google Mail account?
- ☑ **Layout, spelling and grammar:** Is the number of spelling and grammar errors noticeable? Are there unknown characters in the email? Does the layout generally make a high quality impression?
- ☑ **Salutation:** Was I addressed with my real name?
- ☑ **Psychological pressure:** Does the sender threaten to publish video recordings, legal action or similar? Does the sender ask for quick action?
- ☑ **Check links, attachments and websites:** Is the URL the original website address of the alleged sender? What are the file formats of the attachments? Does the phishing website request data that should actually be known to the operator?
- ☑ **Request for confidential data:** If the recipient is asked to enter passwords or PIN numbers requested?
- ☑ **Security measures:**
    - Do I use different and secure passwords for each account? Do I use two-factor authentication? Am I familiar with the typical phishing scams?
    - Emergency measures: Change passwords, have accounts blocked, report phishing attacks to companies and the consumer advice centre

Basically, all of the indicators and tips mentioned above are important for the **detection and prevention of phishing** attacks, but in order to be reliably protected, **Hornetsecurity recommends the use of email security services** that already prevent phishing attacks in advance.