How to identify phishing emails

According to statistics from email security firm MailFrontier, only ... 4% of users are able to identify phishing emails at 100% accuracy rate.

Security threats take place in many forms and scales. You may have heard about viruses, trojans, keyloggers and more recently ransomware. So what do they have in common? All of them can be the result of scams.

Hackers use prey - often in the form of a seemingly legitimate file or link - to "trick" the victim. And because this scam is often spread via email, it is difficult for security software to remove it. So it is very dangerous.

100 billion emails sent every day! See your own inbox. You may have some retail offers, be it updates from your bank or photos from a friend's vacation. Whether those emails come from your online stores, banks or friends, how can you be sure they are not scams?

How to identify phishing emails

What is phishing?

Phishing is a large-scale attack, where a hacker will forge an email and make it appear to come from a legitimate company (such as a bank), often tricking the recipient into downloading malware. or enter confidential information on a phishing site (a website pretending to be legitimate but in fact, it is a fake site used to deceive people to lose their data), where Hackers will be able to access. Phishing attacks can be sent to a large number of email recipients, and as long as a small number of people are trapped, the attack is also successful.

What is spear phishing?

Spear phishing is a type of phishing and often involves a dedicated attack against an individual or an organization. Usually with spear phishing, an attacker will impersonate an individual or part of an organization. For example, you might get an email that seems to be from the IT department saying you need to re-enter your login information on a certain website or from the HR department with 'new benefit packages'. Attached.

1. How to identify a link is safe?

Why is phishing a threat?

Phishing poses a huge threat because it is difficult to identify these types of messages. Some studies have shown that up to 94% of employees cannot find the difference between real email and phishing. Therefore, up to 11% of people click on attachments in these emails, and of course they often contain malware. A recent study from Intel showed that a huge number, up to 95% of attacks on enterprise networks are the result of spear phishing. Spear phishing is clearly not a lightweight threat.

It is difficult for people to recognize the difference between real email and fake email. Although there are sometimes obvious clues such as spelling errors and attachments with the extension .exe, etc.

Even experts have become victims of phishing.

According to a study by Kapost, up to 96% of experts worldwide have been unable to find 100% of the difference between a real email and a phishing email in the past. It is worth mentioning here that even people with a high level of security may be at risk of becoming a victim of phishing. But this rate will be even higher without any security knowledge.

It's easy to create a fake email

This article will show you a simple way to create a fake email, using the SMTP tool (which can be easily downloaded from the Internet). You can create a domain and multiple user accounts from the server or directly from your own Outlook account. For example, you can create an account that is bill.gates@microsoft.com or barrack.obama@whitehouse.gov, or whatever you want.

You can then start emailing these addresses immediately from Outlook. This shows how hackers can easily create email addresses and send you a fake email to steal your personal information. The truth is that you can impersonate anyone and anyone can impersonate you without any difficulty. However, there are several solutions to this problem, including Digital Certificate.

What is Digital Certificate?

A Digital Certificate is like a virtual passport. It tells other users that you are anyone you want. Just like a passport issued by a government, Digital Certificates are issued by Certificate Authorities - CAs. Just like how the government checks your identity before issuing a passport, the CA will have a process called vetting to determine who you are.

There are many levels of censorship. In its simplest form, the CA only checks whether the email is owned by the applicant. At the second level, CA checks the identity (such as a passport, etc.). Higher levels will involve the verification of the company and the individual's actual location.

Digital certificate allows you to digitally sign and encrypt an email. This article will only focus on what it means to digitally sign an email.

Use digital signatures in email

Electronic signing an email makes the recipient think that the email they received comes from a legitimate source.

The sender's verified identity is clearly displayed in the email. In addition to proving the origin of the email, digitally signing an email also has:

1. **Undeniable** : Since an individual's identity is used to sign an email, then they cannot deny that they are not the signatories.
2. **Message integrity** : When the recipient opens the email, their email application checks to see if the content of the email matches the contents of the applied signature. Even the slightest change to the original document will cause this test to fail.

A sad example of a victim of phishing

True story: A few years ago, a public was forced to pay a ransom. Nearly all data files - including Word documents, Excel spreadsheets, etc. - are encrypted and stolen for ransom. Hackers forced this business to pay $ 700 to retrieve data.

According to a hired security expert to help, ransomware infiltrated when someone opened an email attachment, named My resume - a seemingly harmless action, especially when the company is in demand. looking for human resources.

Phishing can also lead to identity theft and even disabling you from your own phone. But won't security software protect you from such threats? Yes, but phishing has a lot of 'tricks' to trick victims: It comes in the form of seemingly harmless emails and forces you to act - often causing you to click on a link or open it. a file, and so

you become a victim of phishing.

While many people already know this and uphold vigilance, there are still many people who can become victims.

How to detect fake email

Below is an example of an email with some phishing signs. The recipient in this example is of a PayPal user.

1. Many people have several email addresses. But this message is sent to an address that is not linked to a PayPal account. Moreover, the " **To** " field is blank, a clear sign that it doesn't really come from PayPal.
2. Grammar and wrong spelling are also signs of phishing. Large companies hire professional copywriters (and editors) to contact via email.
3. The recipient's name is missing. The greeting is merely "Hello, [blank]." PayPal will definitely write the recipient's name in the email.
4. Another important clue to prove this is fake email: This person has never registered this email with PayPal. Now, you might think, "Oh, no, someone created a PayPal account with my name!". This is a tactic designed to help you click the blue call button. After clicking on it, you will be redirected to a site that looks a lot like PayPal, with a form that requires all kinds of personal information - including credit card numbers. In addition, you may be taken to a stealth site, which can install a variety of spyware and / or viruses into your computer / phone.

Here are some pretty sloppy phishing examples. And there are a lot more sophisticated tricks out there, like "Your account has been compromised!" or "FedEx has a package waiting for you" - fraudulent emails cannot be distinguished.

Tips for identifying a phishing or spoofing email

Phishing is spreading more than ever, increasing more than 162% from 2010 to 2014. They make global organizations lose 4.5 billion dollars annually and more than half of Internet users receive At least one phishing email every day.

Companies resist phishing attacks by blocking malicious emails before they reach customers with the Domain-based Message Authentication Reporting and Conformance DMARC standard.

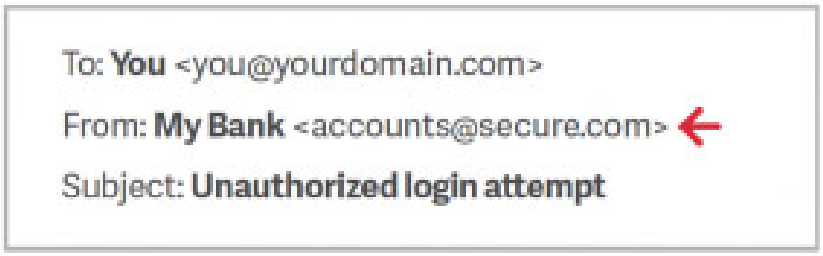
But some phishing emails will still be sent to the inbox. And they are extremely effective - 97% of people globally cannot identify sophisticated phishing emails.

Here are 10 tips on how to identify fake or phishing emails.

Tip 1: Do not trust the display name

A favorite scam tactic of cybercrime is to fake the display name of an email. Return Path analyzed more than 760,000 threatening emails, targeting the world's 40 largest brands and found that nearly half of brand-name emails in the display name.

Here's how it works: If a fraudster wants to impersonate the 'My Bank' brand, email may look like this:



Because My Bank does not own the domain name 'secure.com', DMARC will not block this email on behalf of My Bank, even if My Bank has set a DMARC policy for mybank.com to reject unsolicited messages. This phishing email, when submitted, appears legitimate because most inboxes of users only have display names. Do not believe the display name. Check email address in the title. If it looks suspicious, don't open the email.

Tip 2: See but not click

Hover over any link embedded in the email content. If the link address seems strange, do not click on that address. If you want to check the link, open a new window and enter the website address directly, instead of clicking the link from the email.

Tip 3: Do not lose personal information

Banks are legal and most other companies will never ask for personal login information via email.

Tip 4: Beware of urgent or threatening words in the subject line

Causing a sense of urgency or fear is a common phishing tactic. Be careful with the subject lines claiming 'your account has been suspended' or your account has 'unauthorized login attempts'.

Tip 5: Review the signature

An email lacks detailed information about the signer or how you can contact the company, possibly from a fraudster. Legal businesses always provide contact details.

Tip 6: Do not click on the attachment

Attaching malicious files containing viruses and malware is a common phishing tactic. Malware can damage files on your computer, steal passwords or install spyware without your knowledge. Do not open any email attachments that you did not expect.

Tip 7: Do not trust the title from the email address

Fraudsters not only forge brands in display names but also in titles from email addresses. Return Path points out that nearly 30% of more than 760,000 emails spoof fake brands in headlines from email addresses (the domain alone for email is more than two-thirds).

Tip 8: Don't believe everything you see

Scammers are very sophisticated. An email with a brand logo, language and email address seems legitimate, doesn't mean it's legal. Please question everything. If it looks suspicious, don't open it.

Even if you have security software, phishing is still a serious threat. Here's how to avoid these dangerous emails.

How to prevent phishing emails

Always in doubt: Phishing emails often try to confuse you with warnings about stolen information and then provide an easy fix - you just "click here". (Or vice versa: "You have won a prize! Click here to confirm!"). When in doubt, do not click on anything. Instead, open your browser, visit the company website, then log in normally to see if there are any signs of strange activity. If you are worried, change your password.

Spelling and grammar checking: Most texts are not written by native speakers who have spelling and grammatical errors. But as mentioned earlier, big companies will hire experts to make sure their email has no spelling errors. If you see typos in received emails, it is almost certainly a fake email.

Enhance your browser: An accidental click on a phishing link can lead to a disaster. McAfee SiteAdvisor and Web of Trust are additional free browsers that will warn you if the website you are about to access is suspected to be malicious. They are like traffic police, stopping you before you turn into a dangerous street.

Use your phone: If you are checking email on your phone, it may be really difficult to detect phishing signs. You can't "hover over" a problematic link and a smaller screen makes you less likely to detect clear signs. Although many phone browsers (and operating systems) are immune to malicious websites and download content, it is still prudent to handle suspicious links. (Obviously, you should still not complete a password request form or your other personal information.) Android users in particular need to know about the potential risks.

Most of them are based on intuition: You cannot win a competition that you have never participated in. Your bank will not contact you with an email address that you have never registered. Microsoft will not "detect remote viruses on your PC." Know the warning signs, think before you click and never give out your password or financial information, unless you are logged in to your account properly.

5 paranoia about phishing

MailFrontier's most important contribution in this research result, is that they have pointed out five things people still paranoid about phishing.

1. "Oh, find a trick that is as easy as peeling candy!"

The biggest mistake users have is that they are always too confident in their abilities. Although the level of user awareness of phishing emails has improved a lot, that does not mean that they are alert and knowledgeable at all times to know that they are being cheated. Most of them still equate a phishing email with legitimate email.

2. So the spam filter is a pile of scrap metal?

Most users tend to divine spam filters, saying they can detect and prevent all phishing attacks. And so they are assured, carefree click on every email that appears in their mailbox. Be aware that in order to "catch" a phishing email, there must be a series of complex analysis and evaluation tools, but only a spam filter alone will only know . "laugh except" only.

3. Can phishing email be blocked by domain authentication?

Use domain authentication as a tool to block phishing emails as a third myth. Spammers, as well as professional phishers, have shown they can completely overcome this gate.

4. Is it possible to block phishing email if detecting a URL in the URL?

The vulnerability in the URL address is a good sign to realize that something is not right, but itself cannot do convincing evidence. Many legitimate companies still use techniques such as redirecting URL addresses, using long URLs (exceeding the length of the icon bar) and even raw IP addresses in their emails.

Phishers understand this fact very well, so they took advantage of it.

5. Why do I need to take action to protect myself and my company from phishing emails?

This is the last and perhaps most important paranoia. Users always think that they do not need to do anything, or doing is not helpful. However, this "laziness" can lead to incalculable consequences: loss of personal, financial and confidential data of the company.

According to MailFrontier predictions, the amount of phishers cheated this year will increase by 25% compared to last year to . 1 billion USD.

See more:

1. Beware of phishing emails impersonating Facebook
2. Microsoft shows how to avoid trapping phishing
3. Phishing emails redirect according to the type of sending