The Basics of Phishing

Devolutions

THERE'S A GOOD CHANCE THAT MANY OF YOUR NON-TECHNICAL COLLEAGUES ARE LESS INFORMED

I know that the IT pros who frequent our blog know all about the dangers of phishing. Unfortunately, there's a good chance that many of your non-technical colleagues are less informed. Yes, they probably know a few things. But it's not what they know that will cost them — it's what they DON'T know.

While phishing has been around for a long time, it's not going away any time soon. Here are some pretty scary statistics according to the Verizon Data Breach Investigation Report (DBIR):

- 94% of malware is delivered by email.
- 90% of incidents and breaches include a phishing element.
- 28% of phishing attacks are targeted.
- 21% of ransomware involve social actions, such as phishing.

Plus, a review of multiple surveys and studies by CSOOnline.com found that 56% of IT decision makers feel that preventing phishing attacks is their number one priority.

And so, I thought it would be helpful to put together an article on the basics of phishing. If you're an IT pro, then in addition to refreshing your knowledge (hey, a little review now and then never hurts, right?), I encourage you to share this with your colleagues — so they can make sure they are part of the cybersecurity solution instead of (unintentionally) part of the problem.

What Is Phishing?

Essentially, phishing is an attempt by hackers to disguise themselves as legitimate individuals (e.g. colleagues/friends) or organizations, so that unsuspecting victims end up sharing sensitive information such as passwords, credit card numbers, and so on.

How Does Phishing Happen?

By now, it's highly probable — or make that 100% guaranteed — that you've been targeted by numerous phishing attacks. The vast majority of these have been scooped up your email client's SPAM filter, but occasionally some of them slip through the cracks and can end up in your inbox.

Many of these phishing emails are obvious scam attempts that you can easily spot. But it's a big mistake to assume that all hackers are sloppy or incompetent. For example, in our poll question from last September, we asked our community to share the most realistic-looking cyber scams they've ever seen. Many respondents highlighted phishing emails that appeared to be from legitimate senders such as Amazon, Microsoft, eBay, Apple, credit card companies, and even their own colleagues.

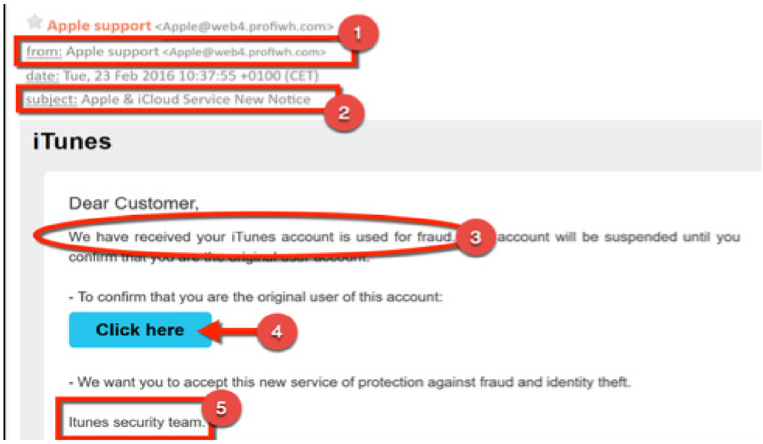
Generally, phishing attacks that use fake websites follow this path:

Step 1 – Targeting

Hackers identify an organization that they plan on spoofing (i.e. pretending to represent). Often, they choose a reputable and trusted organization with a broad client base such as financial institutions, online auction sites, software companies, and large retail chains. Next, they create a copy of the organization's website using the same text, logos, and images found on the original site. Just like the emails, some of these phony websites can look very authentic.

Step 2 – Emailing

Hackers send out an email to a high volume of recipients, or to specific individuals (this is called "spear phishing"). Respondents are directed to click a link, which takes them to the phony website described earlier. Here is an example:



Apple support <Apple@web4.profiwh.com>

from: Apple support <Apple@web4.profiwh.com>

date: Tue, 23 Feb 2016 10:37:55 +0100 (CET)

subject: Apple & iCloud Service New Notice

iTunes

Dear Customer,

We have received your iTunes account is used for fraud. account will be suspended until you confirm that you are the original user account.

- To confirm that you are the original user of this account:

- We want you to accept this new service of protection against fraud and identity theft.

Itunes security team.

1. From: You'll notice that the sender's email address is: apple@web4.profiwh.com, which at first glance looks legitimate because it has the word "apple" in it. Yet even still, many people never bother to look at the actual email address in the first place. They just look at sender, which in this example is "**Apple support**".

2. Subject: This is often something that aims to create a sense of urgency. In this example, hackers use two words that have been shown to increase email open rates: "**Notice**" and "**New**".

3. Content: Usually, the first line in a phishing email is meant to get your heart racing — which impairs your judgment. In this example, the first line is pretty scary indeed: "We have received your iTunes account is used for fraud". Notably, even though the grammar of this sentence is bad, because people are so frightened they tend not to notice. They immediately think, "Oh no, my account has been hacked!".

Also, hackers typically use a generic title instead of a specific name. For example, in this email they use "Dear Customer". This is simply because they're sending the same email to thousands of potential victims. Spear phishing emails will typically use a targeted individual's first name (and also possibly their last name). For example, my SPAM folder is routinely filled with fake emails that start with "Dear Jenny".

4. Action Button: Many phishing emails don't have a traditional looking link. Instead, they have a button, which is the case in the above example. The button is used strategically because people are more likely to click on buttons than links (by the way, this is why you see buttons on landing pages that are selling stuff).

5. Signature: This is often a "team" or "department", although sometimes it can be a (fake) employee's name. In this example, the fake email is from "ITunes security team". Again, the fact that "ITunes" is spelled wrong (it should be "iTunes") is a clue that victims often overlook because they are so freaked out.

Step 3 – Gathering Information & Identity Theft

Once they successfully capture a victim, hackers gather personal and confidential information such as credit card numbers, passwords, PINs, social security numbers, dates of birth, and so on. This information is then used to commit identity theft, such as draining bank accounts, making fraudulent credit card purchases, taking out loans and mortgages, etc.

Phone Phishing

Sometimes, hackers will try to lure victims over the phone. This is called phone phishing (or voice phishing). For example, hackers will claim to be representatives of a credit card company that has detected potential card misuse, and as a result the victim must confirm their credit card number or social security number.

Also, hackers can combine phone and email tactics as part of the same attack. For example, hackers will call a victim who works in the Accounts Payable department of a corporation and pretend to be a vendor who has recently changed banks. The hacker then tells the victim that they will be emailing them the new bank account information. Because the victim immediately sees the email the moment the phone call ends (or sometimes even during the phone call), they believe it must be legitimate. The victim then changes the payment details accordingly. The scam only comes to light when the real vendor complains that they didn't get paid!

What to Do If You've Clicked on a Phony Link

Obviously, you never want to click a phony link and get caught in a hacker's net. But what happens if you do? Well, in most cases, in the immortal words of Douglas Adams from The Hitchhiker's Guide to the Galaxy: DON'T PANIC.

As long as you haven't logged into the phone website or provided any other confidential information, then here is what to do: shut down your browser, clear your cache and cookies, and run an anti-malware scan, anti-virus scan, and anti-spyware scan.

Tips to Stay Safe

Here are some additional tips to help you avoid being victimized by phishing attacks:

- Always Check the URL! Just because the address looks OK, don't assume that you're on a legitimate site. Often if you look closely, you'll notice some small changes, like substituting the letter "l" for the number "1" (e.g. 1inkedin.com instead of www.linkedin.com). Also check and see if the URL starts with http:// instead of https://. A secure website will always start with https://. That extra little "s" is really important! Lastly, look for the little padlock next to the website address.
- Always be suspicious when you receive an email that:

1. Has a sense of urgency and directs you to immediately click on a link or a button.
2. Asks you for personal or financial information.
3. Asks you to change your passwords.
4. Offers a reward in exchange for information.

- Don't click links or buttons in an email. If you think the email might be legitimate, go straight to the company's website and confirm.
- Don't download any attachment that comes from an unknown source. These are often used to spread viruses and malware.

- If you think an email is suspicious, or if you find yourself on a website that seems dubious, contact the sending organization directly. Important: don't phone the company using the number that appears in the email! Believe it or not, the person on the other end could be part of the scam. Find the organization's number from a trusted directory or source.

Basically, the most important thing is to be vigilant. Stay alert, don't assume anything, and follow your instincts — because they're probably right. As Obi-Wan would say: May the Force be with you!