Phishing Attacks: What You Need to Know

Nathan Dinwoodie and Wei Lu
Department of Computer Science
Keene State College
The University System of New Hampshire

Abstract

In this article, we will be discussing the social engineering cyberattack known as phishing. We will go over some examples, the different forms it can take, and why it is a prevalent threat. We will also go through some steps the average user can take to identify these threats and mitigate the damage that they can cause.

1. Basic Phishing Scenarios

Consider the following scenario. A man gets an email that appears to be from his bank informing him that his password will expire in 24 hours and needs to take immediate action. Panicking, the man clicks on the link provided and follows the instructions on the web page, entering his username, previous password, and the new password. However, in his trusting and panic-driven rush, he fails to observe that the email, and the link, are not from his bank but from a cyber criminal who is masquerading as his bank.

Now, armed with the man's login credentials, that masquerader can proceed and complete many transactions before the man or the bank catch up to them. Or maybe the urgent message was not sent to him through his email, but instead, he got a call on his phone informing him about an exciting opportunity that he could be a part of, and all he had to do was provide some personal information. Or perhaps he got a text informing him that the Amazon gift card he just won can be collected by clicking the link provided, despite him not entering any contest.

These scenarios, with an enticing or urgent message sent digitally masquerading as a trusted source, are all examples of the cyberattack known as phishing.

2. Understanding Phishing Attacks?

Phishing is one of the most popular social engineering attacks, where the attacker pretends to be a trustworthy entity to trick the victim. This is done to steal login credentials or the victim's identity, upload malware on their computers, or use ransomware to withhold their data until the victim pays them to get it back.

The unique feature of phishing attacks is that they value quantity over quality. Instead of attacking one victim in a specific way, the goal is to target as many victims as possible.
The act of fishing, which it is named after, is a good analogy for these attacks. The attacker puts out bait that looks trustworthy, the worm on the hook, and hopes that out of a large group, the fish in the lake, at least one, would fall for it.

Phishing is one of the most common types of cyberattacks because of how simple it is to do successfully, due to the skills required being different from conducting other common cyberattacks. This is because it requires more "people skills" than "technical skills" to make the victims fall for the attacks.

3. Types of Phishing Attacks

Phishing attacks come in many different forms, but there are a few prevalent ones that everyone using electronic communication should know about. The first one is email phishing, where, like the first example provided above, the attacker sends the victim an email that looks like it was sent by a trustworthy source so that the victim interacts with it. This is the most common type of phishing attack, accounting for 44% of all attacks, due to the level of detail they can put into the email to make it look convincing.

Two other prevalent forms of phishing attacks are smishing, sent through text messages, and vishing, where the attack is conducted using a phone call. A common theme of these types of phishing attacks is that they are achieved through a digital means of communication. This allows the attacker to reach as many people as possible with minimal effort.

The following two types of attacks are defined not by the form of communication they take, unlike the previously mentioned types, but by their intended targets. They use the fishing analogy in their names that match their description. The first one is spear-phishing, where the attacker targets a specific, but a still broad, group of people such as employees of a company or government organization. This is usually the first step in a more powerful attack, such as an advanced persistent threat. Nearly 95 percent of all attacks on enterprise networks result from successful spear phishing. Due to the smaller scope of targets, phishing is much more difficult but has more rewarding results.

The last type of attack that is most important to know about is whaling, where the target is a high-profile individual like the CEO of a company. They make a lucrative target because their login credentials can often access all the restricted data of an organization since they are the ones in charge. Hence, while it is the most challenging type of phishing attack, it has the most reward.

One thing to be aware of for phishing attacks is that they are the means of how other cyberattacks reach victims and are not dangerous by themselves. They could use things such as malware, ransomware, and spoofing, which will be explained briefly, as they have enough details to be the topics of future articles. The main thing to remember is phishing is the method used to make victims lower their defenses and give away their information or let malicious software onto their system.
4. Tools Used in Phishing Attacks

There are many tools that attackers use to conduct phishing attacks. The first and most important one is the various forms of digital communication, such as email, text, and phone. These allow attackers to target hundreds, or even thousands, of victims easily, with email and text having the added benefit of being able to add links. Another benefit email has is that it can have an attachment of malicious software right in the message, meaning the victim could download it directly to their computer if it convinces them enough to do so.

Another essential tool is the websites attackers created that the links lead to. These websites are made to mimic the trusted site they are impersonating as much as possible and store the information that the victim inputs in them, a practice known as website spoofing. These sites could also host malware such as viruses, worms, ransomware which can infect the victim's computer and potentially lock away their data until they pay the attacker a large sum of money. Interestingly, in 2020, even though more link-based phishing attacks were sent out than attachment-based ones, more people fell for the link-based attacks.

The last and second most important tool used for phishing attacks is social engineering skills, without which the phishing attack would not succeed. These are used to make the victim believe that the attack is trustworthy, encourage them to click the malicious links, and input their information. The most common social engineering tactic used by attackers is making the victim have less time to think logically by making the messages seem urgent, by saying that they need to respond in a short amount of time, or appealing to their greed, like saying they could win a lot of money. This makes the victim overlook possible signs that it is a trick in favor of personal gains or avoiding penalties.

5. Some Recommended Fortification Steps Against Phishing Attacks

There are a few prudent, cautious, and disciplined steps users can take to prevent or lessen the damage from phishing attacks. The first and most crucial step is to take your time and be logical. Attackers use urgent and alluring messages in their attacks to make the recipient gloss over any possible clues or suspicions they might have that it is false. By taking the time to critically look at and think about the details of the messages, we are already taking away a lot of their power. We can ask ourselves some simple questions when we get an email that seems suspicious, such as: "have I ever interacted with this company/organization before?" or "is this offer too good to be true?"

The second step is to be observant; the attack will try to make the message look convincing, but they can't cover everything. Look for spelling mistakes or if it refers to the recipient with something generic that could be used on thousands of people, like "dear customer." The best thing to do is to check the link without going to the site by hovering the cursor over it and checking if the website name that appears at the bottom left of the screen matches it. This is because they can't get a domain name that matches the actual site exactly, so they will try to get something that looks similar, like "Netflix.net."
These tips might help someone recognize a phishing attack and not fall for it, but what to do after? The first thing is to not click on anything in the message; just going on their site could be dangerous. If we recognize that a message is a phishing attack from the title alone, don't even risk opening it.

Next, if you have an account with the company in the news and are not 100% certain it is phishing, contact the actual company differently from what the email or text provides, like looking up the actual site. If it is a legit and urgent message, you can deal with it in a safe, legitimate way. However, if you do not have an account with the company and/or were able to confirm it was a phishing attack, the first thing you should do is forward it to the Anti-Phishing Working group at reportphishing@apwg.org for emails or SPAM (7726) if it is a text. Next, Report the phishing attack to the FTC at ReportFraud.ftc.gov by following the steps on the website.

But let's say you have fallen for a phishing attack; what should you do? The first step is not to panic. Second, if personal information was stolen, go to IdentityTheft.gov and take the specific actions they tell you to do based on which data was stolen. If malware was installed on your computer, run a virus scan with your security software. While this is not a lot, there are actions one can take to minimize the damage if they fall victim to a phishing attack before it happens. The first is having their accounts use two factor authentications, which will make it so that even if the attacker gets their login credentials, they still won't be able to get in. Another action a person could take is to back up all their essential data so that if the attack puts malware or ransomware on their computer, they don't lose anything.

6. Expected Future of Phishing Attacks

The phishing attack is the simplest but perhaps the most effective cyberattack in our current cyberspace. This is because even though all cyber security attacks require a certain degree of technical knowledge, it does not take a lot to get a list of email addresses, send them an email with a link to a web page created, and collect the information entered in.

Two major factors will always make phishing attacks easy and dangerous. First, a chain is as strong as the weakest link, and humans will always be the lowest in a security system. It does not matter if a network has Pentagon levels of security; if someone on the inside messes up, none of it would have mattered. And since there will always be psychological tricks that people will fall for, there is always a chance to mess up.

The second major factor is phishing attacks will always be profitable because it needs to be easy for authorized users to get into the system. There is always a balancing act when it comes to security, where it must be challenging enough for enemies to not get in without being a hindrance for those who are allowed in. So, due to the amount of accessible access user login credentials, they will always be a target. These two factors mean that phishing attacks are not going anywhere, so people must be informed.