Different Types of Phishing Attacks

Phishing involves an attacker trying to trick someone into providing sensitive account or other login information online. All the different types of phishing are designed to take advantage of the fact that so many people do business over the internet. This makes phishing one of the most prevalent cybersecurity threats around, rivaling distributed denial-of-service (DDoS) attacks, data breaches, and many kinds of malware.

Knowing the different types of phishing attacks can equip you to protect your organization from each.

1. Spear phishing

Spear phishing involves targeting a specific individual in an organization to try to steal their login credentials. The attacker often first gathers information about the person before starting the attack, such as their name, position, and contact details.

Example of spear phishing

An attacker tried to target an employee of NTL World, which is a part of the Virgin Media company, using spear phishing. The attacker claimed that the victim needed to sign a new employee handbook. This was designed to lure them into clicking a link where they would have been asked to submit private information.

2. Vishing

Vishing, which is short for "voice phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.

Example of vishing

In 2019, there was a vishing campaign that targeted members of the UK's parliament and their staffers. The attack was part of an assault that involved at least 21 million spam emails targeting UK lawmakers.

3. Email phishing

In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.

Example of email phishing

Hackers used LinkedIn to grab contact information from employees at Sony and targeted them with an email phishing campaign. They got away with over 100 terabytes of data.

4. HTTPS phishing

An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.

Example of HTTPS phishing

Hacker group Scarlet Widow searches for the employee emails of companies and then targets them with HTTPS phishing. When the user gets a mostly empty email, they click on the little link that is there, taking the first step into Scarlet Widow's web.

5. Pharming

In a pharming attack, the victim gets malicious code installed on their computer. This code then sends the victim to a fake website designed to gather their login credentials.

Example of pharming

In 2007, a complex pharming attack went after at least 50 financial institutions across the world. Users were directed to false websites and instructed to enter sensitive information.

6. Pop-up phishing

Pop-up phishing often uses a pop-up about a problem with your computer's security or some other issue to trick you into clicking. You are then directed to download a file, which ends up being malware, or to call what is supposed to be a support center.

Example of pop-up phishing

Users have sometimes received pop-ups saying they can qualify for AppleCare renewal, which would supposedly avail them of extended protection for their Apple devices. However, the offer is fake.

7. Evil twin phishing

In an evil twin attack, the hacker sets up a false Wi-Fi network that looks real. If someone logs in to it and enters sensitive details, the hacker captures their info.

Example of evil twin phishing

A Russian military agency called GRU was recently charged with executing evil twin attacks using fake access points. The access points were made to look like they provided connections to real networks when in reality they led users to sites that stole their credentials or downloaded malware onto their computers.

8. Watering hole phishing

In a watering hole phishing attack, a hacker figures out a site a group of users tends to visit. They then use it to infect the users' computers in an attempt to penetrate the network.

Example of watering hole phishing

In 2012, the U.S. Council on Foreign Relations was targeted by a watering hole attack. The assault aimed to take advantage of the high-profile users that were frequenting the site, as well as the login credentials they could provide. The attack achieved some success, particularly using a vulnerability within Internet Explorer.

9. Whaling

A whaling attack is a phishing attack that targets a senior executive. These individuals often have deep access to sensitive areas of the network, so a successful attack can result in access to valuable info.

Example of whaling

A founder of Levitas, an Australian hedge fund was the target of a whaling attack that led the individual to a fake connection using a fraudulent Zoom link. After following the link, they had malware installed on their system, and the company lost $800.000.

10. Clone phishing

A clone phishing attack involves a hacker making an identical copy of a message the recipient already received. They may include something like "resending this" and put a malicious link in the email.

Example of clone phishing

In a recent attack, a hacker copied the information from a previous email and used the same name as a legitimate contact that had messaged the victim about a deal. The hacker pretended to be a CEO named Giles Garcia and referenced the email Mr. Garcia had previously sent. The hacker then proceeded to pretend to carry on the previous conversation with the target, as if they really were Giles Garcia.

11. Deceptive phishing

Deceptive phishers use deceptive technology to pretend they are with a real company to inform the targets they are already experiencing a cyberattack. The users then click on a malicious link, infecting their computer.

Example of deceptive phishing

Users were sent emails that came from the address support@apple.com and had "Apple Support" in the sender information. The message claimed that the victim's Apple ID had been blocked. They were then prompted to validate their accounts by entering information the hacker would use to crack it.

12. Social engineering

Social engineering attacks pressure someone into revealing sensitive information by manipulating them psychologically.

Example of social engineering

A hacker pretended to be a representative of Chase Bank while saying that the action was needed on the target’s debit or ATM card. The attacker was trying to pressure the victim into divulging their information by leveraging their fear of not being able to access their money in their Chase account.

13. Angler phishing

Anglers use fake social media posts to get people to provide login info or download malware.

Example of angler phishing

Hackers pretended to represent Domino's Pizza on Twitter, fielding the concerns and comments of customers. Once they engaged with a customer, they would use their situation to try to get their personal information—using the guise of trying to get them a refund or a reward.

14. Smishing

Smishing is phishing through some form of a text message or SMS.

Example of smishing

Hackers pretended to be from American Express and sent text messages to their victims telling them they needed to tend to their accounts. The message said it was urgent, and if the victim clicked, they would be taken to a fake site where they would enter their personal information.

15. Man-in-the-middle (MiTM) attacks

With a man-in-the-middle attack, the hacker gets in “the middle” of two parties and tries to steal information exchanged between them, such as account credentials.

Example of man-in-the-middle attack

In 2017, Equifax, the popular credit score company, was targeted by man-in-the-middle attacks that victimized users who used the Equifax app without using HTTPS, which is a secure way to browse the internet. As the users accessed their accounts, the hackers intercepted their transmissions, stealing their login credentials.

16. Website spoofing

With website spoofing, a hacker creates a fake website that looks legitimate. When you use the site to log in to an account, your info is collected by the attacker.

Example of website spoofing

Hackers made a fake Amazon website that looked nearly identical to the real Amazon.com but had a different Uniform Resource Locator (URL). All other details, including fonts and images, looked legitimate. Attackers were hoping that users would put in their username and password.

17. Domain spoofing

Domain spoofing, also referred to as DNS spoofing, is when a hacker imitates the domain of a company—either using email or a fake website—to lure people into entering sensitive information. To prevent domain spoofing, you should double-check the source of every link and email.

Example of domain spoofing

An attacker would execute a domain spoofing attack by creating a fraudulent domain made to look like a real LinkedIn site, for example. When users go to the site and enter any information, it is sent straight to hackers who could use it or sell it to someone else.

18. Image phishing

Image phishing uses images with malicious files in them meant to help a hacker steal your account info or infect your computer.

Example of image phishing

Hackers have made use of AdGholas to hide malicious code written in JavaScript inside images and HTML files. When someone clicked on an image generated by AdGholas, malware would be downloaded onto their computer that could be used to phish for their personal information.

19. Search engine phishing

A search engine phishing attack involves an attacker making fake products that look attractive. When these pop up in a search engine, the target is asked to enter sensitive information before purchasing, which then goes to a hacker.

Example of search engine phishing

In 2020, Google said that they found 25 billion spam pages every day, like the one put up by hackers pretending to be from the travel company Booking.com. An ad would pop up in users' search results that looked like it was from booking.com and included the site's address and the kind of wording users would expect from a real ad by the company. After users clicked, they were prompted to enter sensitive login information that was then transmitted to hackers.