PHISHING

Phishing is a type of cybercrime in which victims are contacted by email, telephone, or text message by an attacker posing as a trustworthy entity in order to obtain sensitive information or data, such as login credentials, credit card details, or other personally identifiable information. Phishing attackers will typically ask for:

- Date of birth
- Social security number
- Phone number
- Credit card details
- Home address
- Password information

An attacker's goal in phishing is to lead the victim to click a link or download an attachment, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or directing users to a malicious website that is disguised as a legitimate site, in which the victim enters in personal information. The results can include large unauthorized purchases, identity theft, and the stealing of funds. Common requested actions in a phishing scam include:

- Clicking an attachment
- Enabling macros in a Microsoft Word document
- Updating a password
- Downloading a file
- Responding to a social media connection request
- Using a new Wi-Fi hotspot

Phishing is a type of social engineering attack, an umbrella term to describe many methods of stealing personal information and manipulation to hack victims' private or corporate accounts. Many scams and cybercrimes fall into the category of social engineering, particularly phishing, but social engineering mainly indicates some level of personal manipulation. Personal manipulation can include calling people over the phone or developing a basic connection with them over social media. Cyber manipulation could mean sending malicious files via email or stealing someone's personal data to access an account or a building. Other types of social engineering includes baiting, scareware, and pretexting.

The term phishing serves as an analogy of the sport of angling. Phishing attackers use "lures," setting out "hooks" to "fish" for credentials and financial data from the "sea" of internet victims.

History of phishing

Phishing is one of the oldest forms of cyber attacks, dating back to the 1990s when AOL was a leading internet service provider. With the large customer base totalling over one million, hackers formed a group known as the warez community, which consisted of people trading

pirated and illegal software and tools, stealing user details, and generating random credit card numbers.

These credit card numbers were used to open new AOL accounts and spam other AOL members, but AOL quickly put an end to this by updating its security measures. AOHell, released in 1995, was a program designed to hack AOL users by allowing attackers to impersonate an AOL employee and send an instant message to potential victims, asking them to verify their AOL account with their credentials.

In 2001, the first direct attack on a financial system was launched against digital currency site, E-Gold, though it was unsuccessful. In 2003, phishing attackers registered domain names that were slight variations of legitimate e-commerce sites such as Flipkart and Amazon. Attackers then sent spoof emails to customers of eBay and PayPal asking them to visit the malicious site and update their password and credit card information.

By 2004, phishing evolved into a profitable business and was officially recognized as a fully organized part of the black market. According to a Gartner study, between 2004 and 2005, an estimated 1.2 million U.S. computer users suffered phishing losses valued at a combined $929 million. One of the primary tactics used by phishing attackers during this was using popup windows to gather sensitive information from unsuspecting potential victims.

What is a phishing attack?

A phishing attack is often broadly aimed at a large number of users. This requires minimal preparation by the attacker, with at least a few targets falling victim to it.

Common examples of phishing attacks

- **Account deactivation**: An email that tells the victim their account has been compromised and will be deactivated unless they confirm their credit card credentials.
- **Compromised credit card**: If an attacker knows that a victim has made a recent purchase, the attacker will send an email disguised as customer support from the company of the recent purchase. The email tells the victim that their credit card might have been compromised and to confirm their credentials.
- **Transfer funds**: An employee receives an email from an attacker posing as the CEO. The fake CEO asks the email recipient for an urgent fund transferral.
- **Social media**: a potential victim accepts a Facebook friend request from someone with a few mutual friends. The newly accepted friend sends the potential victim a Facebook message with a link to a video. When the link is clicked, malware is installed.
- **Google login**: An email posing as Google support claims that they've updated their login credential policy. The attacker asks a potential victim to confirm their Google account information. The senders email is similar to a Gmail address, such as joe.harris@gmail.com
- **Company tech support**: Employees receive an email from their IT department asking them to install new instant messaging software. When employees install the software, ransomware is installed on the company network.

Phishing kits

A phishing kit is a collection of software programs that allows attackers with little to no technical skills to launch a phishing attack. The kit is typically designed to mirror legitimate websites, such as Microsoft, Apple, or Google. A kit includes website development software with a simple, low code or no code graphical user interface (GUI). It offers email templates, graphics, and sample scripts that can be used to create persuasive emails. Most phishing kits are stored on a compromised web server or website, and usually live for approximately 36 hours before being detected and removed.

Types of phishing attacks

Common types of phishing attacks include:

- **Spear phishing**

Spear phishing targets a specific group or type of individuals, such as a company's system administrators. These emails are customized with the target's name, position, company, work phone number, and other information that would trick the recipient into believing they are the sender they claim to be. This kind of phishing is common amongst social media sites such as LinkedIn, where attackers can use different data sources to create a targeted attack email.

- **Whaling**

Whaling targets high-level employees in order to steal sensitive information from a company. A whaling attacker sends a legitimate-appearing email posing as a senior executive such as a CEO or CFO with the aim to manipulate the victim into either authorizing a large amount of funds to be wire transferred or clicking on an attachment or link that installs malware. The goal of whaling is to receive money and/or sensitive company information that gives the attacker access to the company's intellectual property, data, or other information that could be sold.

- **Smishing**

Short for SMS phishing, smishing utilizes Short Message Service (SMS) systems to send bogus text messages. Smishing scams frequently seek to direct the text message recipient to visit a website or call a phone number, at which point the person being scammed is enticed to provide sensitive information such as credit card details or passwords. Smishing websites are also known to attempt to infect the person's computer with malware.

- **Vishing**

Vishing is the telephone equivalent of phishing, short for voice phishing. A vishing attacker often pretends to be calling from the government, tax department, police, or the victim's bank, and tries to convince the victim that there is no other option to fix the spoofed problem than by providing the information being asked of them. Attackers may tell victims that if they don't

respond to the problem, they will face criminal charges, have their bank account shut down, or other, serious consequences.

- **Search engine phishing**

Search engine phishing is unique in that the attacker doesn't bother in sending targeted emails. Instead, the attacker creates a website that offers cheap products and too-good-to-be-true deals. This website is crawled then indexed by legitimate search engines. A potential victim clicks on the website, thinking it's a typical page. This website will encourage users to enter in personal information.

How does Phishing attack happen

- **Step 1: The Information (Bait)**

The first of the three steps of a phishing attack is preparing the bait. This involves finding out details about the target, which can be as simple as knowing that they use a particular service or work at a particular business. This is one of the reasons why data breaches where no 'sensitive' information is compromised can be so dangerous: if a service leaks a list of just email addresses of its users, criminals will be able to know that all the owners of those email addresses use that service and can target them with emails that pretend to be from that service.

In more sophisticated spear phishing attacks, cyber criminals can harvest details from your social media profiles in order to build a highly customized spear phishing message that is highly likely to convince you of its genuineness.

- **Step 2: The Promise (Hook)**

Once the attacker has acquired the necessary information to use as bait, they then need to lay out the hook. In order to actually make the target perform an action, the attacker needs to promise something or scare them into action.
In many scams the hook involves making the target believe that one of their accounts have been compromised, creating a sense of urgency and making the target act quickly - perhaps without thinking. The attacker can then redirect the target to follow a link to a page where they can harvest the victim's details.

- **Step 3: The Attack (Catch)**

The third phase of phishing is the actual attack. The cyber criminal sends out the email, and prepares for the prey to fall for the bait.

What the attacker's next action will be will depend on the nature of the scam. For example, if they used a landing page to gain the victim's email password, they can then log in to the victim's email account in order to harvest more information and start sending further phishing emails to the victim's contacts.

Empower your users to help prevent cyber incidents

Learn how usecure helps businesses drive secure behaviour with intelligently-automated cyber security awareness training.

How to recognize a phishing attack

In order to prevent a phishing attack, it's important to be able to recognize one. Phishing attacks typically have similar features that can be spotted in order to prevent personal information from being stolen, including:

- **Too good to be true**: Avoid announcements or attention-grabbing statements that offer something unbelievable. These phishing scams announce the victim as the winner of a lavish prize even though they didn't enter any contests. If something seems too good to be true, it probably is.
- **Sense of urgency**: Beware messages that tell you to act fast or that you only have a few minutes to respond before dire consequences occur, such as an account being suspended or shut down. Most reliable organizations give you plenty of time to respond and never ask for updated personal details over the internet.
- **Hyperlinks**: A link included in a phishing email is typically made to appear very similar to a reputable company's link. Hovering over a link in an email will show the URL that you will be directed to once clicked on. Instead of clicking on the link, hover over it and inspect it for misspellings. For example, "www.anazon.com" looks similar to www.amazon.com, but clicking on the former may lead to malware being installed on your computer.
- **Attachments**: Don't open any attachments you don't recognize. Attachments sent by phishing attackers often include ransomware or other viruses. The only file that is always safe to click on is a .txt file.
- **Unusual sender**: If the email is sent from someone outside of your organization, it's not related to your job responsibilities, or the domain seems suspicious, avoid clicking links or opening attachments.

How to prevent myself from phishing attacks

Your email provider's spam filter may keep out phishing emails, but attackers are constantly looking for ways to outsmart the filters. Steps to prevent phishing attacks include:

1. Know what a phishing attack looks like. As phishing trends are always evolving, stay up to date with the latest attacks and the key identifiers.

2. Don’t click suspicious links. Hover over links to ensure that the destination is the correct one. If possible, navigate to the intended site by using a search engine instead of clicking on the link.
3. Use an anti-phishing add-on. This add-on will spot the signs of a malicious website and alert you about known phishing sites.
4. Don’t give personal information to an unsecured site. If the URL starts with http://, as opposed to https://, don’t enter any sensitive information or download files.
5. Change passwords regularly. Rotating passwords at regular intervals will not only prevent phishing attackers from gaining access but will also prevent other types of cyber crime.
6. Install firewalls. Firewalls act as a shield between computer and attacker and will reduce the chances of an attacker infiltrating the environment.
7. Don’t click on pop-ups. Pop-ups are often linked to malware. Most browsers allow you to install free ad-blocker software that will automatically block malicious pop-ups.

How can I defend my organisation against phishing attacks?

To protect your business from phishing, it is essential to understand the threat. Why would someone target your business? What data do you hold that’s valuable? What financial transactions do you perform that a cyber criminal could try to get their hands on with a forged invoice?

- **2 Factor Authentication**

Multi-factor authentication is absolutely essential for protecting your accounts against phishing. It adds a second line of defence, meaning that even if you fall for a phishing attack and give away your email password, you’ll still be able to stop the attacker from accessing your account.

- **Security Awareness Training**

As phishing can be carried out in so many different ways, there isn’t a simple technical solution that would be able to stop it. Humans will always be the risk factor when it comes to phishing. This is why training is absolutely essential.

Your employees should be taught how to look out for the signs of phishing, and that they should always exercise extra care when following links from unexpected emails. Enrolling your users on security awareness training courses, will help mitigate the threat of phishing emails.

- **Simulated Phishing**

While employee training is essential, phishing simulation allows you to see how your employees perform when faced with a real-world scenario. Simulations allows your employees to see how easy it is to fall for a phishing email, and is highly effective at raising awareness as employees are far more likely to remember falling for a simulated phishing email than they would simply taking a training course.

Top anti phishing software

Anti phishing software works to identify and block phishing content contained in websites, emails, and other forms of online communication that could be used to access data. The software typically warns the user when it comes into contact with a malicious email or site. This software is often integrated with web browsers and email clients into the toolbar.

Top anti phishing software providers include:

- **Avanan**

Avanan uses machine learning algorithms to catch advanced phishing attacks by identifying indicators of malicious emails, such as the time and location of the email sent and the domain itself. It can detect user impersonation or fraudulent messages by analyzing communication patterns and all historical emails to determine prior trust relations between sender and receiver.

Avanan can deploy quickly within a network environment and is designed to work alongside other third-party security providers.

- **IRONSCALES**

IRONSCALES combines artificial intelligence with human intelligence to identify and remove malicious emails. It offers features such as phishing simulation and training, a phishing emulator, AI-powered indecent response, a virtual SOC analyst, and protection against malware, ransomware, and other cyber attacks. Users can report suspicious emails with a button positioned

inside their email inbox. When a user reports an attack this way, all other users who have received the email will be notified with a banner warning.

- **Proofpoint Essentials**

Proofpoint Essentials uses different security techniques to protect against phishing for SMBs. Proofpoint MLX examines text, image, and attachment content to detect phishing attacks. It can detect malicious URLs and attachments that are known to target smaller organizations. Proofpoint Essentials also provides social media account protection, policy-enforced encryption, data loss prevention, and a filter rules engine for inbound and outbound mail.

- **Agari Phishing Defense**

Agari Phishing Defense uses predictive AI to prevent malicious emails from reaching employee inboxes. It scores every message internally and externally within an organization to defend against low-volume, highly targeted phishing attacks. Agari can block spear phishing and business email compromise (BEC) attacks from already compromised accounts, so they don't spread through the rest of the organization.

Employees can report phishing attacks and threats to Agari, which will then analyze to determine the severity or genuinity of the message. The solution is cloud-based and uses API integration to work with all email gateways such as G suite and Microsoft Outlook.

- **Cofense**

Formerly PhishMe, Cofense is an email security and phishing protection suite that offers security awareness training, employee-sourced threat data, detection and response abilities, and security intelligence. Users can report suspicious emails with an add-on button compatible with Outlook, Gmail, and IBM Notes. It has an automated spam engine to differentiate between known threats and false alarms.

"There are two ways to be fooled. One is to believe what isn't true; the other is to refuse to believe what is true."

$$\begin{pmatrix} Are\ you\ ready\ for\ the\ challenge? \\ \\ https://paneltime.web.app/damncon \\ \\ If\ you\ feel\ that\ you\ can, then\ proceed\ with\ this\ link \end{pmatrix}$$

if you are concluding phishing in a line, we say "What you see isn't the truth and the truth is what you can't see"