What Is a Phishing Email?

A phishing email is a deceptive message designed to trick the recipient into revealing sensitive information by posing as a legitimate entity.

Phishing victims are deceived into believing the request for information is from a trusted source, such as a familiar platform, vendor, colleague, or boss. With good intentions, they respond without hesitation, unaware of the scam.

In phishing emails, cybercriminals often ask for the following information:

- Date of birth
- Social security number
- Phone number
- Home address
- Credit card details
- Login details
- Password (or other information needed to reset your password)

Cybercriminals then use this information to impersonate you, apply for credit cards or loans, open bank accounts, and commit other fraudulent acts.

Some cyber criminals use the information collected in an initial phishing email to launch more targeted cyber attacks, such as spear phishing or business email compromises (BEC), that rely on knowing more about the victim.

How Does a Phishing Attack Happen?

Phishing happens when a victim acts on a fraudulent email that demands urgent action. Examples of requested actions in a phishing email include:

- Clicking an attachment
- Enabling macros in a Word document
- Updating a password
- Responding to a social media friend or contact request
- Connecting to a new Wi-Fi hotspot

Every year, cybercriminals become savvier with their phishing tactics, improve their techniques, and try new methods to deceive and steal from unsuspecting people. Now, you can expect phishing through voicemails, texts, and emails.

Examples of Phishing Attacks

Like everything else on the internet, phishing email attacks have evolved over the years to become more intricate, enticing, and more challenging to spot.

All your users must be familiar with these phishing examples and their different forms to successfully pinpoint and flag suspicious messages in their inboxes.

1. Phishing Email

Phishing emails still comprise many of the world's yearly slate of devastating data breaches. They are designed to appear to come from a legitimate source, like Amazon customer support, a bank, PayPal, or another recognized organization. Cybercriminals hide their presence in little details like the sender's URL, an email attachment link, etc.

2. Spear Phishing

This more targeted phishing email attack relies on data a cybercriminal has previously collected about the victim or the victim's employer. Typically, spear phishing emails use urgent and familiar language to encourage the victim to act immediately.

3. Quishing

Quishing is a new phishing attack that uses QR codes to trick victims into visiting fraudulent websites or downloading malware. It's become quite common nowadays due to the popularity and growing trust in QR codes.

4. Link Manipulation

Relying on carefully worded phishing emails, this attack includes a link to a popular. This link takes victims to a spoofed version of the popular website, designed to look like the real one, and asks them to confirm or update their account credentials.

5. Fake Websites

Cybercriminals send phishing emails that include links to fake websites, such as a known mail provider's mobile account login page, asking the victim to enter their credentials or other information into the fake site's interface. Malicious websites often leverage a subtle change to a known URL to trick users, such as mail.update.yahoo.com instead of mail.yahoo.com.

6. CEO Fraud

This example of a phishing attack uses an email address familiar to the victim, like the one belonging to the organization's CEO, Human Resources Manager, or the IT support department. The email urgently asks the victim to act and transfer funds, update employee details, or install a new app on their computer.

7. Content Injection

Savvy cybercriminals hack a familiar website, including a fake login page or pop-up directing visitors to a bogus website.

8. Session Hijacking

With this advanced phishing attack, criminals gain access to a company web server and steal confidential information stored on it.

9. Malware

In malware attacks, recipients open phishing emails that contain malicious attachments. When clicked, the attachment installs malicious software on the user's computer or the company network. These attachments look like valid files. Sometimes, they're disguised as funny cat videos, eBooks, PDFs, or animated GIFs.

10. “Evil Twin” Wi-Fi

This occurs when free Wi-Fi access points are spoofed. Victims unknowingly log into the wrong Wi-Fi hotspot. Wi-Fi access points commonly spoofed include those available in coffee shops, airports, hospitals, shopping malls, public parks, and other public gathering locations.

11. Mobile Phishing (Smishing)

A fraudulent SMS, social media message, voice mail, or other in-app message asks the recipient to update their account details, change their password, or tell them their account has been violated.

The message includes a link that can be used to steal the victim’s personal information or install malware on the mobile device.

12. Voice Phishing (Vishing)

This scenario occurs when a caller leaves a strongly worded voicemail that urges the recipient to respond immediately and to call another phone number. These voicemails are urgent and convince the victim, for example, that their bank account will be suspended if they don’t respond.

13. Man-In-The-Middle

This sophisticated phishing email attack tricks two people into believing they’re emailing each other. However, the hacker sends fake emails to each person asking them to share information or update confidential corporate information.

14. Malvertising

This phishing technique uses online advertisements or pop-ups to compel people to click a valid-looking link that installs malware on their computer.

Real-World Examples of Phishing Email Attacks

Social engineering tactics are one common thread that runs through all types of phishing emails, including the examples below. Like most phishing attacks, social engineering preys on the natural human tendency to trust people and companies.

This leads many users to fail to carefully review phishing email details and automatically trust the sender’s request. Email phishing victims believe they’re helping their organizations by transferring funds, updating login details, or providing access to proprietary data.

15. Account Deactivation

An email from PayPal arrives telling the victim that their account has been compromised and will be deactivated unless they confirm their credit card details. The link in the phishing email takes the victim to a fake PayPal website, and the stolen credit card information is used to commit further crimes.

16. Compromised Credit Card

The cybercriminal knows the victim made a recent purchase at Apple, for example, and sends an email disguised to look like it is from Apple customer support. The email tells the victim that their credit card information might have been compromised and that they should confirm their credit card details to protect their account.

17. Transfer Funds

An urgent email arrives from the company CEO, who is currently traveling. The email asks the recipient to help the CEO transfer funds to a foreign partner. This phishing email tells the victim that the fund request is urgent and necessary to secure the new partnership. The victim doesn't hesitate to transfer the funds, believing she is helping both the company and the CEO.

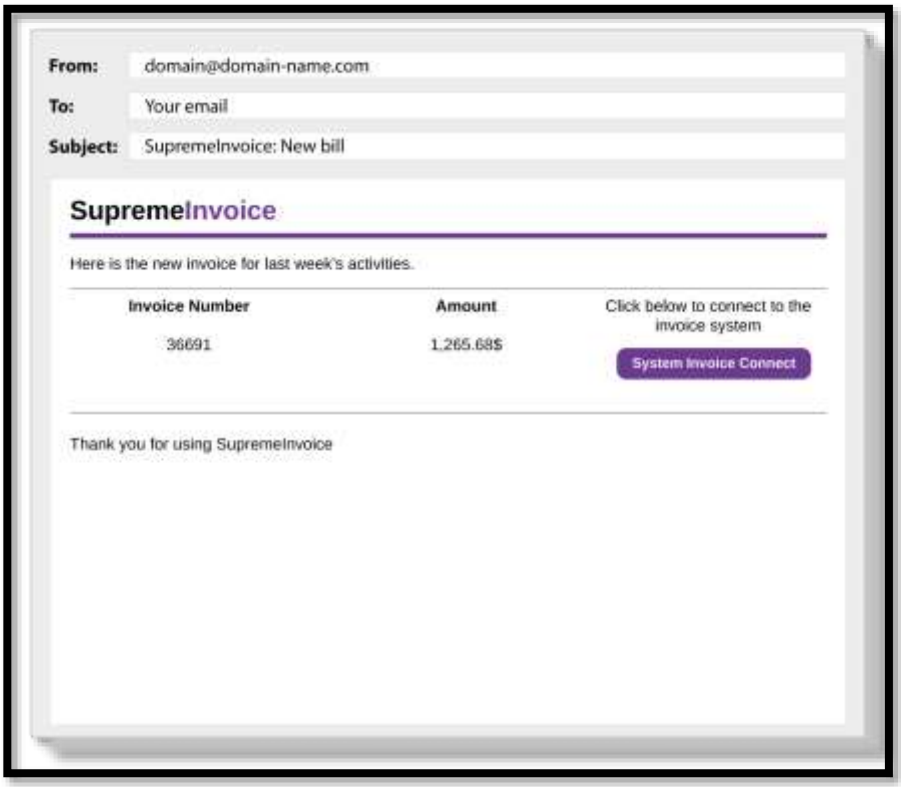
18. Social Media Request

A Facebook friend request arrives from someone who has the same Facebook friends as you. You don't immediately recognize the person but assume the request is legitimate because of the friends in common. This new friend then sends you a Facebook message with a link to a video that, when clicked, installs malware on your computer and potentially the company network.

RELATED READING: <u>COUNTERING THE 5 MOST COMMON SOCIAL MEDIA PHISHING SCAMS</u>

19. Fake Google Docs Login

A cybercriminal creates a fake Google Docs login page and then sends a phishing email to trick someone into logging into the fake website. The email might read something like, "We've updated our login credential policy. Please confirm your account by logging into Google Docs." The sender's email address is a fake Google email address: accountupdate@google.org.com.



From: domain@domain-name.com
To: Your email
Subject: SupremeInvoice: New bill

SupremeInvoice

Here is the new invoice for last week's activities.

Invoice Number	Amount	Click below to connect to the invoice system
36691	1,265.68$	System Invoice Connect

Thank you for using SupremeInvoice

How to Protect Your Data from Phishing Emails

The examples above highlight how cyber criminals can find many ways to trick you into giving information. To protect against phishing attacks, people need to be aware of the various types and know how phishing happens.

The key to prevention is creating a high level of cybersecurity awareness through training and practice. Phishing simulations are an ideal way to train users to identify and avoid phishing attacks.

They show users different types of phishing emails and test their powers of discernment. They give employees first-hand experience with phishing scenarios and demonstrate how easy it is to be tricked by what looks like authentic communication through a valid email.

When people return to real-life scenarios, they're more likely to carefully review emails, URLs, and the context of communication before acting on instinct. Phishing simulations teach people to pause and analyze before automatically clicking "Reply," visiting embedded links or downloading unsecure attachments.

Follow these five steps to protect against phishing email attacks and build cybersecurity awareness in your organization:

1. Educate: Use security awareness training to educate, train, and change behavior.
2. Monitor: Use phishing simulation tools to monitor employee knowledge and identify who in the organization is at high risk for receiving or responding to a phishing attack.
3. Communicate: Provide ongoing communications and run campaigns about phishing emails, social engineering, and cybersecurity.
4. Incorporate: Make cybersecurity awareness campaigns, training, support, education, and project management part of your corporate culture.
5. Apply: As end users, apply this knowledge about phishing email attacks to everyday activities. Be aware of the risks and take the time to assess emails, texts, and websites.