October 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people

Phishing Fundamentals

Securing Your Inbox

Phishing In Every Format

Business Email Compromise

Securing Your Inbox

Email continues to represent the main way cybercriminals launch phishing attacks. Even though modern spam filters can eliminate the majority of spam and suspicious messages, it's up to you to filter out the rest. Here are five ways to secure your inbox:

1. *Know the warning signs*

Phishing scams often feature recognizable warning signs. Poor grammar, threatening language, unrealistic promises, and unexpected attachments all qualify. If a message includes any of these signs, take extreme caution and assume you're being targeted.

2. *Hover over links*

Hovering your mouse over a link will reveal the full URL. This helps you spot malicious links, which usually lead to websites that have nothing to do with the context of the message. Note, however, that even if a link appears safe, it could still be dangerous. Only click if you're absolutely sure.

3. *Don't make assumptions*

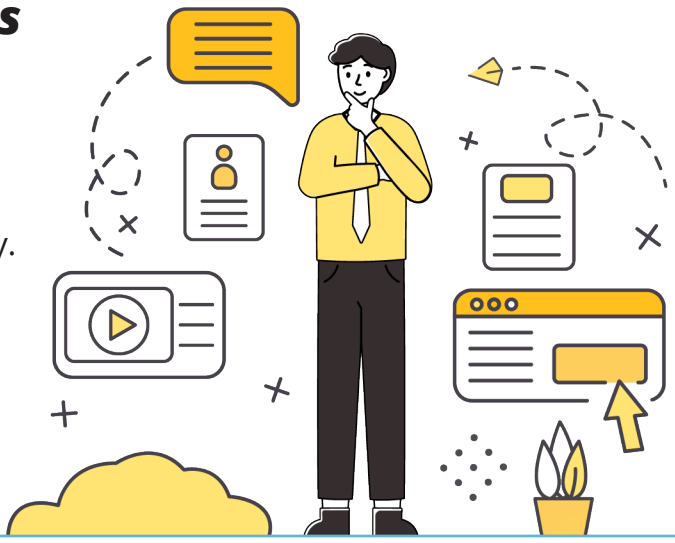
Just because an email appears to come from someone you know doesn't mean it's safe. For example, if a major data breach leaks thousands of usernames and passwords, cybercriminals could use that data to take over people's accounts and distribute phishing emails. Always take note of the tone and context of a message to avoid getting scammed.

4. *Remain skeptical*

There's a fine line between being paranoid and being proactive. We want you to live on the proactive side by treating all requests for confidential information or money with a high degree of skepticism. Follow your instincts, and use situational awareness!

5. *Report suspicious emails immediately*

Any time you suspect an email is a phishing attack, don't click, don't respond, and don't ignore it. Instead, follow policy and report it immediately. Timely reporting allows organizations to analyze the email and take measures to ensure the sender can't distribute additional phishing attacks to your co-workers.



Phishing in Every Format

Email isn't the only way scammers attempt to phish people. They'll happily use every format available to them. Let's explore a few other avenues.

Text Messages

Malicious text messages feature many of the same techniques found in typical phishing attacks. They often claim a bank account has been compromised and ask you to immediately click on a link. Doing so could give a cybercriminal access to personal information or allow them to take over banking and social media accounts.

QR Codes

Many organizations use QR codes as a quick and convenient way to direct users to websites or other services. Scammers also use QR codes to send users to malicious sites that steal login credentials or infect devices with malware. It's generally best to never scan codes unless you're sure they're safe. When in doubt, go directly to a website through a browser app rather than a QR code.

Phone Calls

Since phone numbers are so easy to acquire, cybercriminals have been using them for decades to scam people out of money and personal information. It's a practice known as vishing, or voice phishing. In many cases, vishing attacks use an automated system that asks you to enter banking details. Some attacks will even connect you to a live scammer who will attempt to impersonate legitimate organizations.

Web Browsers

Browser push notifications are small messages that deliver information to users. While push notifications can serve useful purposes, they're also abused by malicious hackers to deliver malicious advertisements or trigger installation of unwanted software. Ideally, block all browser notifications to help avoid this threat.

Regardless of the delivery method, almost all phishing attacks share one thing in common. They attempt to manipulate people into doing something they shouldn't, such as clicking a link, downloading a malicious attachment, and revealing confidential information. Don't fall for it! Use extreme caution before you click, download, or share anything confidential.

Business Email Compromise

Business email compromise, or BEC, is an advanced phishing scam that impersonates people, organizations, or entities that the victim knows. It works by manipulating email addresses so the sender appears to be legitimate.

Common examples of BEC:

- **Fraudulent Invoices**
  By impersonating vendors or other account representatives, scammers can trick people into wiring funds to fraudulent accounts. This is often accomplished by sending fake invoices that look almost exactly like an invoice the victim typically receives.
- **CEO Fraud**
  How likely are you to respond to an email that appears to come from your boss? CEO fraud involves a cybercriminal attempting to impersonate upper management and sending out requests for wire transfers of money or confidential information.
- **Account Takeover**
  When someone falls victim to a phishing attack, they may lose control of their email account. This then allows the attacker to distribute phishing emails to the victim's contact list. Since the recipient recognizes the account, they are likely to engage with the attacker.
- **Employee Data Theft**
  Those who work in bookkeeping or human resources have access to an abundance of employee information. Cybercriminals often target those people in hopes of stealing data such as full names, national ID numbers, home addresses, and phone numbers.

You can thwart these attacks by slowing down and:

- **Carefully inspecting the sender's email address.**
  Scammers often create addresses that appear to be legitimate but actually contain slight variations in the way they're spelled.
- **Paying attention to the tone.**
  When you email regularly with someone, you are likely familiar with how they communicate via text. Unusual tone = untrustworthy email.
- **Avoiding attachments.**
  Email attachments represent one of the most common ways malware gets distributed. Never open an attachment unless you have confirmed it's safe.
- **Verbally confirming.**
  If you receive a request for money or confidential information, it's always a good idea to confirm with them via an alternative method before complying.