



HOW TO SPOT A PHISHING SCAM



Phishing attacks are one of the most common forms of cybercrime and are a critical threat to any organization, especially as social engineering attacks become more sophisticated and difficult to identify. The best way to prevent a phishing attack is to know how to identify a phishing email. The following product provides simple tips for recognizing a phishing scam disguised as a legitimate email.

BE CAUTIOUS OF GENERIC EMAILS

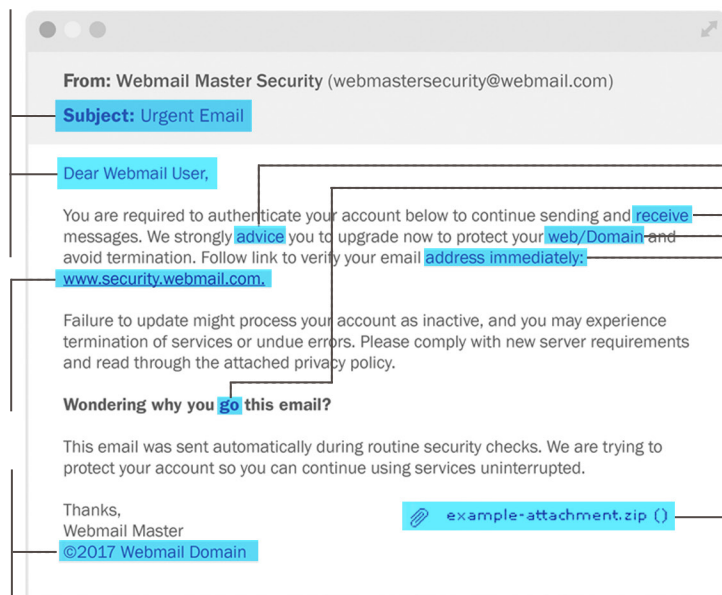
Phishers try to cast a wide net by including little or no specific information in their fake emails. Always be wary of messages with generic subject lines or messages that don't contain your name, last digits of your account number or other personalizing information.

SUSPICIOUS URL

Hover over links included in emails to see the actual destination of the URL.

IMPROPER USE OF COPYRIGHT

Watch for improper use of copyright information. This is used to make the phishing email look official.



BAD GRAMMAR/SPELLING

Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

UNNECESSARY URGENCY

Use your intuition and if something feels wrong, consider calling the organization or office directly to validate the email.

SUSPICIOUS ATTACHMENT

Phishing emails may contain attachments containing malicious code. Avoid opening attachments that seem suspicious or come from a sender you do not know.

TYPES OF ATTACKS

DECEPTIVE PHISHING

The most common form of phishing in which a cybercriminal impersonates a legitimate organization to lure the recipient into revealing sensitive information or click on a link/attachment that infects the user's computer with malicious code.

SPEAR PHISHING

Spear phishing is when a cybercriminal targets specific individuals in a phishing attempt. Cybercriminals may gather personal information about their target – often using information gleaned from social media – to customize the phishing attempt.

WHALING

Whaling is similar to spear phishing, only the target is bigger; in whaling attacks the cybercriminal targets executive officers or senior managers in an organization. Whaling emails are often customized – frequently containing personal information and company logos.

OTHER METHODS

The widespread use of Dropbox and Google Docs by organizations has led cyber criminals to customize their attacks to target users of these platforms. Voice phishing – or vishing – is when a fraudster uses the phone to solicit sensitive information instead of email.

"NCSAM Phishing Awareness 2017 Poster"
Department of Homeland Security, 25 September 2017

PHISHING SCAMS

USERNAME:
PASSWORD:

PHISHING PREVENTION TIPS

The following are some simple best practices from the Department of Homeland Security and Better Business Bureau to help prevent you or your organization from falling victim to a phishing attack:

When in doubt, throw it out:

Links in email and online posts are often how cybercriminals compromise your computer. If it looks suspicious – even if you believe you know the source – it's best to delete or, if appropriate, mark it as "*junk email*." Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. Contact the company directly (*via phone*) to be sure the email is not legitimate.

Think before you act:

Be wary of communications that implore you to act immediately, make vague threats, offer something that sounds too good to be true, or ask for personal information.

Use stronger authentication:

Always opt to enable stronger authentication when available, especially for accounts with sensitive information, including your email or bank accounts. A stronger authentication helps verify a user has authorized access to an online account. For example, it could be a one-time PIN texted to a mobile device, providing an added layer of security beyond the password and username.

Make passwords long & strong:

Combine capital and lowercase letters with numbers and symbols to create a more secure password. Change passwords periodically.

Install & update anti-virus software:

Make sure all of your computers are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

Be wary of hyperlinks:

Avoid clicking on hyperlinks in emails; type the URL directly into the address bar instead. If you choose to click on a link, ensure it is authentic before clicking on it. You can check a hyperlinked word or URL by hovering the cursor over the displayed hyperlink to reveal the full address.

Be wary of attachments:

Avoid opening attachments in emails from senders you are not familiar with. Attachments can download malware onto your computer and/or steal your identity. If you choose to open an attachment, ensure it is authentic before clicking on it.

Be cautious of what you share on social media:

Consider only connecting with people you already know. Be sure to use privacy settings on all social media and online accounts. Cybercriminals often get information about their targets from their online interactions and profiles, and they can use that information to make their phishing attack more convincing and increase their chances of tricking their target.

Use secure, traceable transactions:

Do not pay by wire transfer, prepaid money card, gift card, or other non-traditional payment method when making payments for goods, services, taxes, and debts.

Be wary of sharing personal information:

Never share personally identifiable information with someone who has contacted you unsolicited, whether it's over the phone, by email, on social media, even at your front door.

