7-Step Guide to Avoid Email Scams

Stay Vigilant with Your Email

Be vigilant about opening and responding to emails. When receiving an email from a subscription service (even your bank), the best practice is to visit the source directly using a new web browser to verify if the message is accurate. Never click a link from an email. Most legitimate organizations will not email you directly with instructions to change your password or provide login credentials. You will always receive emails for deals and specials, but many businesses are turning to internal notification systems for updating sensitive information.

Always stop and think.

Recognize Threats by the Tone Used

Cybercriminals will usually take an alarmist or threatening tone in phishing emails. They want to induce panic and a sense of urgency so that the recipient will click and enter information without thinking. The criminals use this to their advantage.

Always stop and think.

Don't Give Out Information via Email

Users should be very cautious of emails that suggest entering any personal information. If in doubt, the user should reach out directly to that organization to verify the accuracy of the message. Legitimate organizations don't typically ask users for personally identifiable information through email.

Always stop and think.

Inspect the Email Address

Pay attention to how closely a domain name (in the email address) could resemble a website you frequent. **www.paypal.com** looks very similar to **www.paypa1.com**. Cybercriminals are intelligent and will buy domain names that resemble a company because it is similar enough to trick someone.

Always stop and think.

Never Download or Open Attachments

Do not download files or click links in an email, even if they come from a seemingly trustworthy source. Unless you are expecting an email with an attachment, it is best not to click or download. This tip is good to use even when you are at work, where you may expect to receive emails with attachments from colleagues. Always confirm with your colleagues before opening anything.

Always stop and think.

Be a Grammar Nazi

Watch out for grammatical errors in the body of the email and the subject line. While no one has perfect grammar, the simple mistakes in many malicious emails are usually a dead giveaway that you are being phished! Many cybercriminals are from other countries, and English is not their first language, so their mistakes are very obvious.

Always stop and think.

It Looks Phishy and Smells Phishy...

Clearly, you should always stop and think. However, what is the next step? If you think you may have received a malicious email, start by asking yourself the following questions:

- Why am I receiving this email?
- What is it asking me to do?
- What is the sender's email address (not just the sender's name)?
- When hovering the cursor over the link (text or image). What is the website URL show that you will be visiting when you click?

If the answers to these questions are **suspicious** in any way, don't click, don't download, don't take any action instructed in the email. Block the sender, and mark the email as "junk."

Staying safe online is part of everyday life today. We must all pay attention to what we are doing online—email is no different.

Help your entire office stay safe.
Download our Security Best Practices Poster here.

BW BitWizards

BITWIZARDS.COM | (850)226-4200