Don’t fall for these phishy tricks

Common phishing tactics

Phishing emails are one of the most common cybersecurity threats. With about 319 billion emails sent and received each day, users need to be on high alert for phishing attacks.

According to Proofpoint’s 2021 State of the Phish report, 75% of organizations around the world experienced a phishing attack in 2020. 74% of attacks targeting US businesses succeeded.

But knowing that phishing emails are out there and dangerous is not enough. It’s important to be able to recognize one. Take a look.

Urgent message

An urgent phishing email is designed to get you to act fast. It might tell you that your account was hacked or is going to be deactivated — click here to restore it! Unfortunately, urgent phishing messages are common because they work. Fear makes people do things without thinking, so slow down!

Login or password message

Another type of phishing email asks you to verify your account by logging into a (fake) webpage or clicking a button to update your credentials. These types of emails can collect your username and password, giving a hacker instant access to your account.

Internal message

Hackers will try to impersonate someone at your company, real or fake. They might impersonate someone in the HR department, IT department or even a coworker. In an internal message phishing email, it might ask you to click on a link to read and sign a policy document, read a document about a company-wide update or even try to request sensitive information.

Reward or free gift message

Free things are enticing, but they can also be dangerous. If you get an email saying you won a free TV or “click here to enter a prize drawing,” be on high alert! Hackers are trying to bait you into clicking a malicious link.

Help! I might be getting phished. What should I do?

If you think you have received a phishing email, it’s important to slow down and examine it. First, look at the sender and domain of the email address. Hover over any links and see where they might direct you to. Other phishy identifiers might be misspelled words, incorrect dates or odd requests. If you see anything, report it to your IT department. They can help you figure out if it’s a phishy email. Whatever you do, do not click on any links, reply to the email or send it to anyone else!

International Computer Security Day (November 30th)

We are one click away from anyone on the other side of the globe. Because of this, a cybersecurity incident in another country could still affect you. Celebrate International Computer Security Day with these four simple security tips:

- Audit and update all of your passwords. For added security on your personal devices, use a trusted password management tool. Reminder: Don’t use the same password more than once!
- Use multi-factor authentication on your devices and accounts. This will give you an extra layer of security.
- Enable automatic updates on your devices. Keeping your devices up to date keeps you one step ahead of any hackers.
- Share these tips with your friends, family and colleagues! Knowledge is power, and the more people know about cybersecurity, the safer everyone will be.

Phishers attack at many levels

Everyone is at risk of phishing, no matter where they are in the food chain. Phishers specifically target CEOs and high-level executives with special phishing attacks intended to entice or fool them. These are known as whaling attacks.