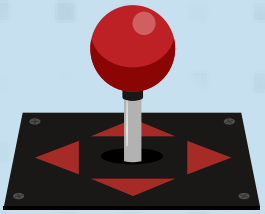
LEVEL UP YOUR CYBERSECURITY

Recognizing and reporting phishing

Cybercriminals sent over 3.3 billion phishing messages and caused over 4,000 data breaches, exposing over 22 billion personal records. But it isn't enough to simply know that phishing emails are out there; you also need to be able to recognize and report them.



Look at some of the highly used phishing email types and tactics

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.

Urgent message

An urgent phishing email is designed to get you to act fast. It might tell you that your account was hacked or will be deactivated — click here to restore it! 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 updating your credentials. These emails can collect your username and password, giving a hacker instant access to your account.

Internal messages

Hackers will try to impersonate people at your company, such as someone in the HR department, IT department or even a coworker. An internal message phishing email might ask you to click on a link to read and sign a policy, read a document about a company-wide update or even hand over sensitive information.

If you think you may have encountered a phishing email, follow your company's procedures for reporting. Once the right people are notified, they can help you determine if it's a phishing email. Whatever you do, do not click on any links, reply to the email or send it to anyone else!