

# Phishing

## **When criminals go phishing, you don't have to take the bait.**

Phishing is when criminals use fake emails to lure you into clicking on them and handing over your personal information, or installing malware on your device. It's easy to avoid a scam email, but only once you know what to look for.

## **See it so you don't click it.**

The signs can be subtle, but once you recognize a phishing attempt you can avoid falling for it. Here are some quick tips on how to clearly spot a fake phishing email:

- Contains an offer that's too good to be true
- Language that's urgent, alarming, or threatening
- Poorly-crafted writing with misspellings, and bad grammar
- Greetings that are ambiguous or very generic
- Requests to send personal information
- Urgency to click on an unfamiliar hyperlinks or attachment
- Strange or abrupt business requests
- Sending e-mail address doesn't match the company it's coming from

## **Oh no! I see a phishing email. What do I do?**

Don't worry, you've already done the hard part which is recognizing that an email is fake and part of a criminal's phishing expedition.

If you're at the office and the email came to your work email address, report it to your IT manager or security officer as quickly as possible.

If you're at home and the email came to your personal email address. Do not click on any links (even the unsubscribe link) or reply back to the email and JUST DELETE IT. You can take your protection a step further and block the sending address from your email program, too.

## **Let them know.**

Some email platforms let you report phishing attempts. If you suspect an email is phishing for your information, it's best to report it quickly.