

# 6 Tips to Avoid Phishing Scams

## 1 Exercise caution.

Don't open emails from unfamiliar email addresses or contacts. If you receive an email that appears to be from a trusted source, but appears 'odd' call and verify with the sender the authenticity of the email.

## 2 Avoid clicking on links & attachments.

Verify a link by hovering your mouse button over the link to see where it leads. Sometimes it's obvious the web address is not legitimate. But keep in mind phishers can create links that closely resemble legitimate addresses.

## 3 Do not use open, unsecure Wi-Fi.

Never use public wi-fi. When working remotely it is best to have a mobile wi-fi device that you can securely connect to.

## 4 Never reveal personal or financial information.

Never provide your log in credentials, financial, or personal information to emails you do not recognize. Always go to websites of trusted sources to enter your information.

## 5 Ignore urgency and take your time.

Phishers love to push urgency in their attacks. Never take immediate action with an email if sensitive data is at risk. Always take your time, remain suspicious, and analyze the email from top to bottom.

## 6 Report suspicious items to your IT department.

If you receive a suspicious email, forward the entire email as an attachment to your IT team. If you click on a link or open an attachment in a suspected phishing email, report any incident immediately.

