

7 Tips to Avoid Being Phished!



Many companies that fall victim to security breaches or virus attacks need look no further than their own employees to find how they were breached. Review the following steps to help educate your employees on how to avoid clicking on the wrong items.

1. *Keep your email, web, and endpoint security up to date.* Take advantage of security software alerts when evaluating the safety of an email, link, or download.
2. *Even trusted email senders can be compromised.* With over 864 million personal data records compromised through data breaches since 2005, you can't always guarantee that an email from someone you know is legitimate. It could be from a scammer impersonating one of your coworkers or friends. So before downloading content or following a link, verify with the sender that they actually sent the email.
3. *Colleagues may innocently send infected links or files to download.* Even if it's really your colleague that sent the email, there's a chance that they've been infected, have out-of-date security software, or ignored an alert. If your security software warns you that the link or download is malicious, don't click or download the content.
4. *Just because an email looks good doesn't mean it's legitimate.* Beware of emails that are badly formatted or contain misspellings—especially from well-known companies. But, keep in mind that just because an email 'looks right' doesn't mean it is right. Smart phishing scams can look virtually identical to legitimate messages.
5. *While some email addresses are obviously from a phony third-party site, it's easy for sophisticated scammers to make an email address look similar to a legitimate domain.* Use caution and assume the email could be a phishing email—even if the sender looks legitimate.
6. *Like email addresses, creating fairly convincing URLs is easy for sophisticated scammers.* Hovering over (long-pressing on mobile) links in email can identify obvious fakes, but many phony URLs are made to be convincing. Some security software will check URL safety for you, but when in doubt, use a search engine to find the actual URL yourself.



7. *Your safest choice is to always stay in the driver's seat by finding content yourself.* If you click a link without a security tool in place to scan URLs in real time, you are allowing that link to pull you to wherever it wants to take you—whether it's safe or not. The extra 10 seconds it takes to search for a site yourself is worth the effort—it can save your company from hours of device repair, protect your sensitive information, and even prevent ID theft. Trusted parties will never ask you for sensitive information in an email. An ounce of precaution is worth a pound of cure.

Feel like you can spot a fake email or phishing scam? Try taking this helpful online quiz from McAfee which provides a variety of examples and explanations about how to tell the difference.

<https://phishingquiz.mcafee.com/>

