Best Practices to Avoid Being Phished

Phishing emails can be difficult to spot. Here are some tips to help you identify and avoid common scams.

1.

KEEP YOUR SECURITY SOFTWARE UP TO DATE

Don’t avoid downloading important updates, hackers exploit vulnerabilities found in older software, so it’s important to keep the apps on your devices current.

2.

BE AWARE OF EMAIL REQUESTS WITH HIGH URGENCY AND QUICK ACTION

If you are ever in doubt, double check the request with the sender either by phone or by composing a new email—never reply to the email itself.

3.

NEVER GIVE PERSONAL OR FINANCIAL INFORMATION OVER EMAIL

Trusted parties will never ask you for personal information through email. Try to make it a company policy not to collect employee information internally via attachments.

4.

DON’T CLICK ON LINKS FROM MESSAGES THAT CONTAIN MISSPELLINGS

If an email from a well-known company is formatted badly, has obvious misspellings or is unrelated to the product or company, this is a red flag.

5.

IF AN OFFER SEEMS TOO GOOD TO BE TRUE, IT PROBABLY IS

Big bonuses, large payments or gifts (ex. win a free iPad) for services are ways attackers try to get inside your head. If the promise is “too good to be true”, do some research before taking action.

6.

THINK ABOUT WHETHER YOU INITIATED THE ACTION

Phishers will try to spoof well-known companies, always be suspicious of unsolicited email, for ex. if you didn't prompt a password reset--don't click the link.

7.

BE CAREFUL ABOUT WHAT YOU POST PUBLICLY TO SOCIAL NETWORKING SITES

If your social networking profile is public, avoid sharing birthdays, kids’ names, or detailed business information because attackers will use it to get clues about what your passwords might be.

8.

STAY EDUCATED ON PHISHING TECHNIQUES

Commonly, these attacks look like urgent emails coming from a boss or colleague, and attachments tend to look like a voicemail, fax or shipment tracking slip.

9.

ACT QUICKLY

If you accidentally click on a link or think that you have been phished, talk to your IT department, put a stop on a wire transfer or alert other people in the organization — immediately.