How to Spot a Phish

Finding the phish 101 with Professor Troy

Lesson 1: Watch out for emotions

Greed

Phishing emails often dangle a financial reward of some kind if you click a link or enter your login information. If an email offers you something that seems too good to be true, it probably is.
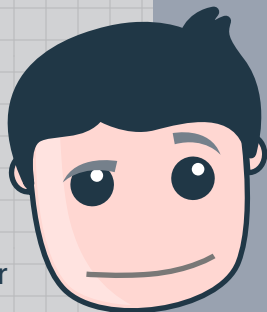
Urgency

If an email provides a strict deadline for performing an action -- be suspicious. Phishing emails will try to fluster recipients by creating a sense of urgency.
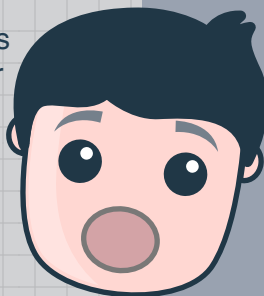
Curiosity

People are naturally curious, and phishers take advantage of this by sending emails that promise to show us something exciting or forbidden.

Fear

Scaring recipients is a common tactic in phishing emails. Emails that threaten you with negative consequences or punishment should be treated with suspicion.

Lesson 2: Examine these items closely

Email Signatures

A signature block that is overly generic or doesn't follow company protocols could indicate that something is wrong.

Bob Jones
IT Manager
Acme, Inc.
(555) 555-5555

Sender Address

If the address doesn't match the sender name, be suspicious of the entire email.

From: Bob Jones <e34grhgshfd @phishing-

Email Tone

We know how our co-workers and friends talk, so if an email sounds strange, it's probably worth a second look.

Greetings Friend,

Please to click on link for

Lesson 3: Beware of these elements

Attachments

When an attachment comes from someone you don't know or if you weren't expecting the file, make sure it's legitimate before opening it.

From: Joe Smith
To: Troy Foster
Subject: WebMail Migration

Attachment -- Webmail_Migration.pdf

Troy,
This is to inform you that we are in the processing of migrate our email infrastructure to the Windows 2003 platform, which includes an e... e-mail.

Attached is a document outlining the benefits of th... migration we request you to enter your Windows password before 8 PM on Tuesday. Failure to do so will result in being locked out of your email account!

Please click here to update your password.

Thank You,
John Smith

Log-in Pages

Spear phishers will often forge login pages to look exactly like the real thing in order to steal your credentials.

Links

Roll your mouse pointer over the link and see if what pops up matches what's in the email. If they don't match, don't click.

If you see something, say something!

Report suspected phishing emails to the information security team.

PHISHME