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 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.

**Sender Address**
If the address doesn’t match the sender name, be suspicious of the entire email.

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

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.

Troy,
This is to inform you that we are in the processing of migrating to the Windows 2003 platform, which includes an email.

Attached is a document outlining the benefits of the migration. To ensure timely 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 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.