EMAIL SECURITY

- Being a Detective
  What to look for

- Phishing
You’ve got email.

Is it spam?
Is it a phishing attempt?
Or is it malware?

It used to be malicious messages were sent by teenage hackers or by solo criminals working by themselves. Things have changed.

Today, organized crime sends many of the malicious emails, and those emails are increasingly sophisticated.

So how do you tell the good email from the bad?
First, running anti-malware software on your computer and/or network is a must. It will catch most of the malicious email.

But software can’t catch everything.
That’s where you come in!
You must develop email detective skills to be able to tell good messages from malicious ones.

Observe
Ask yourself these questions when you examine an email:
- Do you know the sender?
- Did you expect the email?
- Did you expect an attachment?

Investigate
Next look for clues of malicious or spam messages:
- Is the From address an alias?
- What’s the sender’s address?
- Are there many or strange typos, or wording that doesn’t make sense?
- Does the email warn that something bad will happen or promise gifts?
- Where do the message links go? Is it a safe website?

Deduce
Put it all together:
- Are there danger signs?
- Do you need to read it?
- Any doubts, report it to your IT Department or Help Desk. At home, just delete it.
Email Headers
The first step in deciding whether an email is malicious or spam is to observe the email header. If the email is suspicious, delete it.

It's best to view email with preview turned off.
Email clients provide options to see an entire message or a small preview as soon as the email arrives. This is dangerous because even if you don't click on a link or open an attachment, malware can execute from hidden code or images. In Microsoft Outlook, turn off the Reading Pane and AutoPreview.

Exposing malicious emails.
The From (sender) address of a message shown in your inbox can be an alias, even fraudulent. You can often identify malicious emails without opening the message by looking at the email header. For currently supported versions of Microsoft Outlook, here's how to do it:

- Outlook 2010 and 2013 require some configuration to be able to see email headers but it's simple to use once configured. Click here to learn how.
- In Outlook 2007, right click a message, select "Message Options", then look at the "Internet headers" section.
- Check with your IT support staff if you use a different email client or need help.

Game Instructions
On the next page, you'll be presented with an email inbox belonging to Tracy Smith. Decide whether each email in Tracy's Inbox is "Safe", "Malicious", or "Can't Tell".

Observe
Read each email header (To, From, Subject).
Look for obvious warning signs like an incorrect recipient address.

Investigate
Examine the From address. Is it an alias? Roll over it with your mouse. What is the sender's email address?
Compare the senders to Tracy's relationships by clicking the "Tracy's Relationships" button. Look for other clues.

Deduce
Decide whether the email is "Safe", "Malicious", or "Can't Tell" by clicking one of the radio buttons.
You must decide the safety of all of the email headers before you can proceed to the next page in the lesson.
These are the companies that Tracy does business with:

- Tracy shops at these online stores: Macy's, Amazon.com, REI, Petco.
- Tracy has a mutual fund at Fidelity Investments and receives monthly account statements. She does not do online banking.
- Tracy sells books on Half.com and has a PayPal account.
- Tracy has joined the LinkedIn network and gets regular updates about her new connections.
The Email Body
You examined the email header and decided the email looked safe to open. Now examine the email body (text). Look for these clues of malicious emails. Roll over each to see an example:

- **General or Missing Greeting**. Legitimate senders know you and will use your name.
- **Typos and grammar errors**. Sure, some typos are to be expected. But there shouldn’t be too many or ones that wouldn’t be accidentally typed.
- **Incorrect or confusing text**. The words or phrases in the message are confusing when you read it. Or the information is just incorrect.
- **Directed to do something**. You are ordered to take action: log into your account, change your password, or verify your information.
- **Bad things will happen**. You are warned to take immediate action or else you will suffer some consequence.

- **Too good to be true**. You will get something for free, be given special access, or be one of only a privileged few.
- **Suspicous links**. Links displayed in an email can be named to trick you into going to malicious websites. Roll over links to see where they really go.
- **Attachments**. Malicious attachments are often named to look legitimate. Never open attachments that you don’t expect. Scan attachments with anti-malware software before opening.

Let’s talk about link (URL) safety.
Never click on a link in an email unless you know that the real destination is a safe website. First, determine the real URL, not the alias: either read the email in plain text, or roll over HTML links with your mouse so that the URL is displayed.

Next follow these three steps to determine where the web address really goes.

1. Starting at the beginning of the address, http:// or https://, find the first SINGLE “/”. Tell me more
   
   ![http://www.youtube.com/videos?c=19](http://www.youtube.com/videos?c=19)

   First single "/"
2. Next, find the "Site Name". It's the two parts of the web address just to the left of the first single "/". These two parts are separated by a period.

http://www.youtube.com/videos?c=19

Site Name

Carefully look at the "Site Name" and be sure it goes where you want to go.

For example, your bank is mybank.com, but the link goes to mybank.us, which is similar but a malicious link.

3. The part of the web address preceding the Site Name accesses a specific area on a website. However, cybercriminals often use Phony Site Names to make malicious sites look legitimate. So always look at the Real Site Name, just to the left of the first, single "/".

https://chaseonline.chase.com\1867zebrtgo.info/security/login.html

Phony Site Name  Real Site Name

For example, the above address appears to go to Chase Bank but it really goes to "1867zebrtgo.info". If part of a link seems to be phony or deceptive, don't click on it. It may well be malicious.
Game Instructions
On the next pages, you will be shown three malicious email messages. In each are clues revealing that it is malicious.

- Drag and drop a red flag over each clue by clicking on a flag, holding down the mouse button and dragging the flag over a phrase that is a clue, then dropping the flag by releasing the mouse button.
- If dropped over a malicious clue, the flags will stick. A pop-up window will open, describing the malicious clue. The email clue text will be highlighted in yellow.
- An incorrectly dropped flag will return to its original position.
- Flags that don’t stick but display gray highlighted text are informational and not clues.
- You must correctly place all the red flags before you can proceed to the next page.
- For help, click the following buttons: “Hint” to briefly see a single email clue highlighted, “Email Clues” for a reminder of clues to look for in an email, or “Instructions” to see these instructions again.
Reading Email Safely: Observe, Investigate, Deduce

Email Header (To, From and Subject):
- Examine the email's header before opening the message.
  - Read email with Reading Pane and AutoPreview turned off
  - Reveal the sender's email address
  - Identify and delete emails with suspicious email headers
    - You don't know the sender
    - The To (recipient) address in your Inbox appears incorrectly or is missing
    - The From address is an alias and the sender's address doesn't look legitimate
    - Email subject doesn't make sense to you

Email Body:
- Once you determine the header looks safe, you can open the message. Now examine the text in the message body.
  - Identify and delete emails with suspicious text:
    - Email greeting is very general or non-existent
    - There are odd typos in the text or the sentences don’t quite make sense
    - The email message plays on your emotions (e.g., fear)
    - Links in the email go to an address that looks wrong or is unknown to you
  - Never click on a link unless you know what the destination is and that it's trustworthy
  - Don't unsubscribe from emails you didn't sign up for; this just tells the sender that your email address is good
Fishing

Nope, not that kind . . .
. . . this kind

Phishing
Phishing

Phishing, like its namesake “fishing,” uses bait to lure a target into getting hooked. In phishing, the bait is a clever message and you are the fish. Why does phishing matter? Phishing is one of the most successful cyber attacks.

Phishing Messages

A phishing message can arrive by email, phone, social networking message, instant message (IM), or fax. The message will ask you to take an action like clicking on a link and entering information on a website, or calling a phone number. Whatever the message, the goal is to get you to reveal private information like your password, account number, or birth date.

Log in
But why do we fall for it? Why do we take the phishing bait?

Phishers are masters of disguise, making malicious messages look legitimate. You learned about their methods of disguise in the Email Security lesson.

How else do phishers trick us?
They play on our emotions and desires.

Let's take a look at how phishers manipulate our emotions, and see some examples of the words used in actual phishing messages.

Roll over each image
Spear Phishing
Spear phishing is a more sophisticated form of phishing that targets you directly. Messages appear to come from someone you know and trust (e.g., your company, your bank, a friend). They often include personal information like your name, where you live, or your employer. But in fact, it's a spear phishing attack.

Because the messages look so real, it is even easier to get tricked. The massive Target data breach was the result of a spear phishing attack.

To identify spear phishing messages, always look at the sender's address (review the Email Security lesson) or the REAL destination of any links. Remind me how I do this.

Remember, NEVER give away private information in response to a message.

Phishing Clues
You can spot phishing attempts by looking for the new clues that you learned in this lesson, combined with those you learned in the Email Security lesson.

Roll over each phishing clue to read more about it.

- Emotional manipulation
- Asked for private information
- Missing recipient address in email
- Alised sender address
- General or missing greeting
- Typos and grammar errors
- Incorrect or confusing text
- Directed to do something
- Phishing links
Game Instructions
On the next lesson pages, you’ll be shown three different types of phishing attacks. Your task is to identify the clues that reveal why each is a phishing attack.

- Drag and drop a red flag onto each clue. Click on a flag, hold down the mouse button and drag the BASE of the flag over a phrase that is a clue. Then drop the flag by releasing the mouse button.
- If you drop a flag on a real clue, the flag will stick, and the text will be highlighted in yellow. A pop-up window will open with more details about the clue.
- An incorrectly dropped flag will return to its original position.
- If a flag doesn’t stick but displays text highlighted in grey, the text is informational, not a phishing clue.
- You must correctly place all the red flags before you can proceed to the next page.
- For help, click the following buttons: “Hint” to briefly see a single phishing clue highlighted, “Phishing Clues” for a list of clues, and “Instructions” to see these instructions again.
No Phishing Here

Remember, phishers use all of our modern media for their attacks: email, IM, social networks, phone, and even faxes.

- NEVER give out sensitive information unless you initiated the communication and you are sure you have the correct party.
- Be suspicious when a message plays on your emotions: Curiosity, Fear, Trust, Need, Generosity, or Desires.
- Delete messages that:
  - Ask for private information.
  - Display an aliased sender’s address that is not the real sender and looks suspicious.
  - Have suspicious links that don’t go where the aliases say that they go.
  - Don’t click on links (URLs) or call phone numbers provided in messages. Instead, look them up yourself.
  - Investigate any link before you click on it. Phishers often hide a malicious link among several legitimate ones.

Help, I Think I Was Phished!

Despite your best efforts, you think that you were phished. What should you do now?

At Work:
- Stop what you are doing.
- Immediately report the incident to State of Indiana. It may be embarrassing, but the quicker you tell someone, the less damage that might be done.

At Home:
- If you gave away a password, change it immediately.
- Jot down everything you can remember about what happened.
- Call the account provider (e.g. bank or store) and tell them exactly what happened. Refer to your notes.
- If you are the victim of identity theft, have credit bureaus (Equifax, Experian, TransUnion) put fraud alerts on your credit reports.
- Close any accounts that were tampered with.
- Report incidents to the police and Federal Trade Commission (FTC).
Beware Of Phishing