Phishing – Internet Fraud Scam

About the scammer

- Pretends to be a reputable person or organization.
- Sends email messages that appear to be from financial institutions or credit card companies that try to trick recipients into giving personal or financial information.

Other related terms:

- Spear phishing – Targets a selected group of people
- Whaling – Targets executives

Be Careful!

Review email messages

✓ Check the headers
- Someone you know or bogus sender?
- Sent to bogus list?

✓ Check the subject
- Immediate action required?

✓ Check the body of the message
- Generic greeting used?
- Immediate action required?
- Misspellings and grammatical errors?
- Includes links or attachments?

Stop, Think before you Click!

Trust your instincts!

IT Security

How to Spot a Phishing Email

Don't forget, You are the target!

IEEE

Common Phishing Scams

Business Email Compromise (BEC)

- Fake wire transfer requests
- Often targets “Money people” who have authority to make a payment or wire money

IRS Scam

- Request a refund in your name/SS#

Tech Support Scam

- Caller pretends to be from Microsoft or other vendor
- Attempts to have you send them money or let them control your computer

Holiday & Charity Scams

- Often at Christmas or after a disaster – Bogus money requests

What to Watch for?

Watch out for misspellings or unknown senders

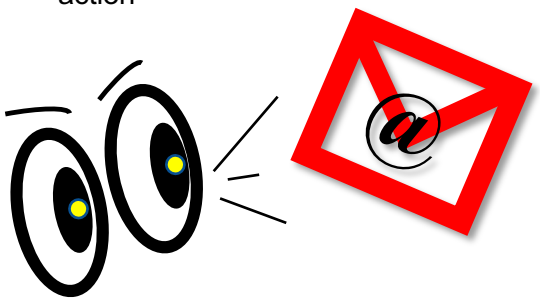
- Legitimate business names are missing or the name of the business is misspelled
- Unexpected email from an address you have never communicated with before

Watch out for email sent to an unknown email address and pay attention to subject lines

- Example: To: payroll@companyxyz.com
- Careful with “too good to be true” offers or threatening statements (meant to elicit emotional reaction)

Watch for generically addressed message (Dear Customer) and its content

- Especially the ones regarding a personal account, financial information or threatening legal action



Watch out for links or attachments included in the message

Hover over the the link to see where the URL would actually take you, if clicked

Scammers will try to implant real business names in the URL

In all circumstances unexpected attachments should not be opened.

These points do not represent all the ways in which scammers will attempt to phish you.

You are the one who has the best understanding of what sort of email messages you usually get at home and at work.

If an email just feels ‘off’ for any reason, that’s enough to be wary of it.