How to Recognize Email Scams

Spam	The email version of junk mail. This is mail that you did not ask to receive and usually is trying to sell you something. Spam emails are sent to a huge list people.
Phishing	Using email as a lure to "phish" around for someone's personal and financial information.
Spoofing	Forging an email address so that it appears to be coming from someone else.
Cybersquatting	Cybercriminals sometimes register web addresses (also called "domain names" or "URLs") that are similar to the web addresses of popular websites or are common misspellings of popular websites. For example, instead of www.microsoft.com, cybercriminals might create a web page with the address: • www.micrsoft.com • www.micosoft.com • www.mircosoft.com
Nigerian 419 scams	The scammer will email you an elaborate fake story about large amounts of money 'trapped' in central banks and needing your help to release it. They may ask for your bank account details to 'help them transfer the money' and use this information to later steal your funds. Or they may ask you to pay fees, charges or taxes to 'help release or transfer the money out of the country' through your bank. Named Nigerian 419 because first emails of this type came from Nigeria—now they can come from anywhere.

Hover, Don't Click

- Hover over the FROM email address (move your mouse there but don't click) and you will be able to see if the email address matches who it is from.

- Be careful about clicking on links within emails. Hover over any links (without clicking) to see where the link is really taking you.

Watch Out For

- Strange email addresses.
- Grammar and spelling errors.
- Strange wording of emails—broken English.
- Strange symbols within the email.
- Threats that if you do not act quickly, bad things will happen such as your account being shut down.
- Emails from overseas—many internet crimes come from other countries.
- Urgent messages. Email scams will often sound very urgent. They may state that you only have 24 hours to respond.
- Scare tactics. The email will be so upsetting that you won't think logically and may click without thinking.
- Sad stories asking for money.
- Unexpected money—emails about inheritances from deceased relatives.
- Visit www.snopes.com to see if an email is real or a hoax.
- Emails from friends that only contain a link and no message.

Safety Tips

Before entering your credit card or other payment type, make sure that the URL ends with an S for secure, meaning your information is safe from identity thieves: Example: **https://**

Report email scams to your ISP, Internet Service Provider or to the company that the email was supposedly from.

Never respond to an email scam yourself.

Never click on any links that may be from an email scam.

Tips and reporting email scams:

U.S. Computer Emergency Readiness Team: https://www.us-cert.gov/report-phishing

FBI's Internet Crime Complaint Center, IC3: http://www.ic3.gov/default.aspx