Spam:

- Any unsolicited message or posting that is sent to multiple recipients, or multiple postings of the same message sent to newsgroups or listservers. It is the electronic equivalent of junk mail.

Prevention:

- Avoid giving your personal email address to anyone you don't know.
- Before registering on a web site, read the site's privacy policy to ensure that your email address will not be shared or sold to a third party.
- Never display your email address openly online, such as in chat rooms, or in profiles.
- When forwarding emails to others, copy and paste the text into a new email before sending. Simply clicking "Forward" also forwards the email addresses of the prior recipients of the email.
- Do not publish your personal email on social networking sites (Facebook, Instagram, etc.)
- Check with your Internet Service Provider to see what spam-blocking utilities it offers and how to activate them.
- Never respond to spam. Ignore the "unsubscribe" links in spam email. If you respond to the email, you are essentially validating that your email address is active and being read. Professional spammers will subsequently sell your email address to other spammers.
- The United States has enacted the CAN-SPAM ACT. You can report spam emails to spam@uce.gov.

Phishing:

- Identity thieves often "phish" for information by sending email spam or pop-up messages that appear to be legitimate businesses (i.e. bank or online payment services). These phishers lure their victims to counterfeit web sites that appear to be the legitimate sites. However, they are intended to trick you into giving up information needed to steal your identity.

Prevention:

- Watch for bad spelling and grammar errors. A scammer often makes spelling and grammar mistakes that would otherwise be caught by a legitimate company's proofreaders.
- Be aware of generic greetings. Most companies you already do business with will address you by name or username. "Dear Valued Customer" should raise a red flag.
- Look out for account suspension or cancellation warnings. They will try to scare you into supplying your information.
- Never directly respond to pop-up messages or emails asking for personal or financial information. Contact the organization via telephone or type the company's web site in yourself.
- Never click on links within emails. Type the address in yourself. Phishers will create links that look like legitimate web sites, then take their victims to phony web sites. In the following example, the two web sites look the same, but change the font and you can see one site has a number 1 instead of a letter l:

- Paypal.com Paypal.com
- Paypa1.com Paypa1. com

- Be cautious about opening emails or attachments, or downloading files from emails, even if they appear to be from someone you know. Scammers often spoof email addresses to trick victims into believing they are receiving emails from someone familiar.

- Never use email to provide personal or financial information to an organization.

- Use antivirus, spam filters, pop-up blockers, and antispyware software to further protect your system.

- Install a firewall.

- Act immediately if you believe you have been hooked by a phisher. Notify your financial institutions immediately and don't forget to contact the credit bureaus and request a fraud alert on your credit files.

Geneva Police Department

20 Police Plaza
Geneva, Illinois 60134
Phone: 630-232-4736
Fax: 630-232-7711

http://www.geneva.il.us/index.aspx?nid=213

Detective Sullivan
Detective Duncan

Internet Safety

Email Threats