west protect

SAFE Tip Sheet
Spam & Phishing

Dec 2019

SPAM is the electronic equivalent of junk mail. The term refers to unsolicited, bulk – often unwanted – email. Spammers send their messages to hundreds, thousands or even millions of email addresses at once with the hope that at least a few people will respond.

One of the differences between Spam and Phishing is that spammers don't attempt to acquire sensitive information for malicious purposes. However, they may collect contact information to add to their databases for future use. It can be annoying, but it's not malicious.

Here are ways to reduce spam:

- *Enable filters on your email programs*: Most internet service providers (ISPs) and email providers offer spam filters. It's a good idea to occasionally check your junk folder to ensure the filters are working properly.
- *Report spam*: Most email clients offer ways to mark an email as spam. Reporting spam will also help to prevent the messages from being directly delivered to your inbox
- *Own your online presence*: Consider hiding your email address from online profiles and social networking sites or only allowing certain people to view your personal information.

PHISHING attacks, on the other hand, use email or malicious websites (clicking on a link) to collect personal and financial information or infect your machine with malware and viruses. This information is then used to access important accounts and can result in identity theft and financial loss.

Protect yourself with these familiar tips:

- *When in doubt, throw it out*: Links in email, tweets, posts and online advertising are often how cybercriminals try to get your information. If it looks suspicious, even if you know the source, it's best to delete or – if appropriate – mark it as junk.
- *Think before you act*: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- *Make your passphrase a sentence*: A strong passphrase is a sentence that is at least 12 characters long. Focus on sentences that are easy for you to remember. On many sites, you can even use spaces!
- *Unique account, unique passphrase*: Having separate passphrases for every account helps to thwart cybercriminals.
- *Lock down your login*: Enable the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passphrases are not enough to protect key accounts like email, banking and social media.

Spam & Phishing on Social Networks:

Spam, phishing and other scams aren't limited to just email. They're also prevalent on social networking sites. The same rules apply on social networks: ***When in doubt, throw it out.*** This rule applies to links in online ads, status updates, tweets and other posts.