Phishing emails are socially engineered emails designed to get users to divulge private information including credit card numbers, passwords and other confidential information. They are extremely convincing that they are from a legitimate source, such as PayPal, a bank, a university or even the IRS.

Detecting a phishing scam is done by being aware of some of the techniques used to collect information from unsuspecting users. One such example is an email supposedly from Gmail stating that your account has been compromised and needs the password reset. This is a common approach, as we all dread to hear that our account has been compromised. It creates a sense of urgency and desire to “click here” and update our account. These are very common. In all cases, do not click any link in the email. Always visit the site as you normally would to change your password. In all cases, be wary of any email directing you to click a link to change your payment, account, or other personal information.

When phishing attacks were first noticed, the fake web sites were usually crude representations of the real sites, but now these sites will usually look exactly like the real thing. These are usually banks, payment services, or other financial institutions. When a user logs in with a username and password or provides payment information, the information is captured and used to impersonate the victims.

Click cautiously: When reading emails, always click cautiously any links in emails. In all cases, be certain you are clicking on links in an email from someone you trust. Beware of any links in emails from any financial institutions, online services (Gmail, Hotmail, Yahoo!, etc.), and commonly known businesses in general, especially if it regards providing information or logging into an account.

Change passwords regularly: Because email is inherently insecure to begin with, it is always a good idea to change online passwords regularly. About every three months or any time you have any concerns on your account security. Also, it is best to use unique passwords for each site you access, since it would be easy to access many online resources with just one compromised password. It can help to use a good password manager like LastPass, Dashlane, KeePass, or RoboForm. Not only do they usually simplify logging in, but are great at generating secure passwords for sites you visit.

Use a good phishing filter and antimalware software: Many recent browsers now support phishing filters for web sites, as well as software vendors like TrendMicro, McAfee, Symantec and others. It helps to use more than one, since there is no perfect solution to the problem.

Use good sense: When reading emails, use good sense and think things through. Does it seem too good to be true? It probably is!

The U.S. Department of Homeland Security National Cyber Alert System has additional tips to help you avoid phishing and other socially engineering scams and attacks.