Fraud Prevention

Safeguard Your Email

Email is often a vehicle used to transmit malware and commit fraud. It is important to evaluate your email behaviors and develop good habits to help protect your computer and your identity.

In addition to viruses and worms that can be transmitted via email, phishing also threatens email users. A type of email fraud, phishing occurs when a perpetrator, posing as a legitimate, trustworthy business, attempts to acquire sensitive information like passwords or financial information.

Never Open or Respond to SPAM (unsolicited bulk email messages).

Delete all spam without opening it. Responding to spam only confirms your email address to the spammer, which can actually intensify the problem.

Never click on links within an email.

It's safer to retype the web address than to click on it from within the body of the email.

Don't open attachments from strangers.

If you do not know the sender or are not expecting the attachment, delete it.

Don't open attachments with odd filename extensions.

Most computer files use filename extensions such as ".doc" for documents or ".jpg" for images. If a file has a double extension, like "heythere.doc.pif," it is highly likely that this is a dangerous file and should never be opened. In addition, do not open email attachments that have file endings of .exe, .pif, or .vbs. These are filename extensions for executable files and could be dangerous if opened.

Never give out your email address or other sensitive or personal information to unknown web sites.

If you don't know the reputation of a web site, don't assume you can trust it. Many web sites sell email addresses or may be careless with your personal information. Be wary of providing any information that can be used by others for fraudulent purposes.

Never provide sensitive information in email.

Forged email purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal information for fraud. It is not recommended to include personally identifiable information in an email. Examples of this include social security numbers, driver's license and other government identification numbers, and account number(s).

Don't believe the hype.

Many fraudulent emails send out urgent messages that claim your account will be closed if sensitive information isn't immediately provided, or that important security needs to be updated online. The Fraudster is trying to pressure the recipient to provide information. Your financial institution will never use this method to alert you of an account problem.

Be aware of poor design and/or bad grammar and spelling.

A tell-tale sign of a fraudulent email or web site includes typos and grammar errors as well as unprofessional design layout and quality. Delete them immediately.

Backup your sensitive data records.

Consider backing up all sensitive files. This will not only help you restore damaged or corrupted data, but it will help protect against fraud attacks and help recover lost files if needed.