Learn about . . .

Spotting Fraud Emails

Below are four red flags that can help determine if an email is legitimate.

1. **Spelling and bad grammar**

   Legitimate companies employ copy editors to review content before circulation, so there should be no spelling or grammatical errors. Cybercriminals, on the other hand, tend not to worry about such niceties. Beware when you see misspellings or other grammatical inaccuracies.

2. **Links in emails**

   Look before you click. Whenever an email contains a link that you want to access, before you click to open it, hover your cursor over the link to see if the addresses match. If not, refrain from clicking the link.

3. **Threats**

   One sign that may indicate a phishing scheme is receiving a threat, such as, "Your account will be closed if you don't respond by clicking the link below." Another red flag is alerts that your security has been compromised.

4. **Spoofing companies and websites**

   These are e-wolves in sheep's clothing. Often, cybercriminals will place logos and other imagery belonging to the companies they're impersonating into the message body, then link those images to their malicious scam sites. If you do click on an image and are brought to the supposed site, look closely at the URL. Some scammers will use an address that closely resembles the URL of the company they're looking to imitate; an example would be http://www.applle.com. You can also use the hovering maneuver with images.

What to do if you have been subjected to a scam

First, report it to your manager or IT staff if you work in a business, or to the police if it happens at home. Most importantly, if you have been a victim, change all PIN numbers and passwords on any accounts, even those that haven't yet been compromised. Contact your bank or online merchant if threats were issued saying your account has been compromised. Call your financial institution and have a fraud alert placed on your credit reports. If your account has been accessed, cancel those accounts and open new ones. Continue to closely monitor your account statements for unexplained transactions.