DON'T BE FOOLED!

Protect Your Network!

1. **Inaccurate grammar or punctuation.** Check the subject line or body for poor grammar or punctuation or an illogical flow of content. This is most likely written by an inexperienced scammer and should be deleted.
2. **Unknown sender address.** Some addresses will look familiar. Hover over that email until you can view the entire email address of the sender.
3. **Asking for personal information.** Any messages asking to enter or verify personal data or bank/credit card information should be treated as big red flags!
4. **Content full of warnings and potential consequences.** If the message causes alarm telling you your account has been hacked, expiring or some other extreme condition that causes you to panic - don't take immediate action. Typically, such emails lead the users to data harvesting sites that end up stealing valuable personal or financial information.
5. **Offers of financial rewards**. The actual intention is usually to direct you to a site where the scammers will get your personal and financial information.
6. **Login and password information.** Having the same User name and Password for several accounts, is convenient, but hazardous. Every bank account, credit card and shopping site should have a different User Name and Password. In addition, do not store this information on your PC.
7. **Invest in an anti-phishing software.** Since scammers are constantly evolving, software is not 100% effective, but still a viable option, and works great in conjunction with the manual prevention listed above.

ANY EMAIL COULD BE A TRICK, SO CHECK BEFORE YOU CLICK!

EMPLOYEE TRAINING

- Educate employees on recognizing Business Email Compromise
- Run drills on identifying Phishing attempts
- Adhere to payment work-flows, protocols and systems
- Trust your gut – many fraud attempts have been prevented because something didn't "feel right"

RED FLAGS TO SIGNAL POTENTIAL FRAUD IN BUSINESS EMAIL

- Email grammar
- Payee Changes
- Urgency
- Contact information change
- Suspicious documents
- Account verification

RANSOMEWARE VULNERABILITIES

- Outdated software
- Unrestricted user access
- Ineffective firewall
- Unscanned email and wesbites

NETWORK COMPUTER Solutions

655 51st Street • Marion, IA
(319) 247-7223 • ncsei.com