**Phishing Awareness Best Practices**

According to the 2017 *Verizon Data Breach Investigations Report*, phishing e-mails account for about **90 percent** of all cyber attacks. To better protect your information against cyber threats, it's crucial to understand the signs of a phishing e-mail.

**Signs of a phishing e-mail**

- **Unexpected requests.** If you receive a request out of the blue—one that you don't regularly handle—it's likely to be a phishing e-mail.
- **Urgency.** Most phishing e-mails prompt recipients for action ASAP; that way, there's not enough time to process what they're reading and doubt its veracity.
- **Poor grammar, spelling, or syntax.** Typos and strange syntax are common features of malicious e-mails.
- **The hover-over link doesn't match.** If you hover over a link within an e-mail and the URL doesn't match the description of the link, it might be a malicious website. **Do not click it.**
- **Asking for sensitive information.** Phishing e-mails often ask you to "verify" your credit card number, social security number, or account password. Never share sensitive information through e-mail.

**What to do**

- **Do not investigate unfamiliar links.** If the e-mail concerns an online account that you log into regularly, simply open up a new browser window yourself and log in as normal.
- **Delete the e-mail.** Do not forward suspected phishing e-mails to anyone. Although reporting phishing e-mails seems helpful, forwarding them increases the chances that a malicious link will be clicked.
- **Call the sender.** If you're unsure, verify the e-mail's veracity with the sender. Don't use a number provided from the e-mail because it could be fake. If you don't know the legitimate number, try researching the official website of the business or individual.