Cybersecurity Awareness Month

Phishing Scams

Subject Line: Beware of Goblins, Ghouls, and Phishing Scams

Dear Employees,

The holiday season is around the corner. For most of us, it is a time of joy, cheer, excitement, and hopefully some relaxation. For cyber criminals, however, this is the busy season (same goes for Santa and his elves).

Cyber criminals use the holidays to take advantage of employees' generosity and more relaxed nature to **TRICK** them into various phishing scams. This is no **TREAT**.

This is your friendly holiday reminder to **BEWARE** of phishing scams and to stay alert.

What is a phishing scam?

Phishing is a type of attack in which individuals are contacted by email, telephone, or text by someone posing as a legitimate business or person to lure them into: (1) providing sensitive data such as personal information, banking and credit card details, and username/passwords, or (2) clicking on a link or downloading an attachment that could provide the cyber criminal(s) with access to the individual's device and systems (including the employer's systems).

What types of phishing scams might you encounter this holiday season?

1. **Charity schemes**
   An email or text asking you to donate to a charitable cause by clicking on a link and asking for payment.

2. **Gift cards purchase**
   A request to purchase gift cards on behalf of the organization to gift to others. Let it be known that our CEO will not be asking anyone to purchase Target or any other company gift cards on his/her behalf. Unfortunately, the budget is tight this year.

3. **Package notifications**
   A fake message from a shipping company, such as UPS or FedEx, informing you that your package has shipped or is ready to be delivered. These types of messages typically include a link for you to click on that may download malware to your device or redirect you to a site asking you to input your personal information.

4. **Temporary holiday jobs**
   Boss not paying you enough and now you're looking for a side gig? Lots of businesses hire

during the holiday season. Be careful when clicking on job advertisements or when sharing your personal information.

5. **Too-good-to-be-true deals**
   With Black Friday around the corner, there will be an increase in marketing and sales advertisements. If a deal looks too good to be true, it probably is. Be careful when clicking on advertisements and when browsing online.

How to spot one

1. **Hover over the link.**
   There are two parts to a link in an email message or a web browser:
   a. The part you see: the words describing the link (e.g., “Google”) or the web address (e.g., www.google.com).
   b. The part you don’t see: the URL the link actually leads to.

   These two things are not always the same. Be sure to hover on the link (without clicking on it) to ensure the part you see matches where the link will take you.

2. **Review the sender’s email address.**
   Be sure to check the sender’s email address and domain name (don’t just rely on the name being displayed).

3. **Be suspicious if someone is requesting personal information, payment details, or login credentials.**
   Businesses will rarely ask you to confirm your personal information out of the blue or through an unsecure method.

4. **Take caution if urgent action is requested.**
   Creating a false sense of urgency is a common tactic used by cyber criminals. Take time to ensure the request makes sense and the message is legitimate.

5. **Be on the lookout for poor spelling and grammar.**
   While the occasional typo is expected in emails, take caution if you see one too many.

6. **Out of the ordinary**
   If the email is out of the ordinary for any of these reasons or others, it may be a phishing scam. Review the list above to see if there are any other flags.

If you receive a phishing email

1. **DO NOT click on any links or attachments in the suspicious email.**

2. **DO NOT forward the suspicious message to anyone else.**

3. **Report the message immediately to** Insert Name/Department **at** Insert Contact Method **.**