HIPAA HIGHLIGHTS

February 2023

E-mail Security

As we have noted in previous *HIPAA Highlights*, URMC and its Affiliates are constantly under attack by malicious e-mail, sometimes referred to as phishing. Some messages we get are obviously illegitimate with many grammatical errors, spelling mistakes, or are just generally incoherent. URMC has protections in place to help protect our users and our data, but you, our workforce members, are still our best line of defense.

The organization has increasingly seen some messages specifically for URMC to look like our internal communications or linked to sites that mirror our internal sites. Additionally, URMC has seen an increase in the number of malicious emails requesting the purchase of gift cards. Remember that you should always verify emails like these out of band (e.g., via phone, in person, etc.) to ensure the request is legitimate. At this time of year, other common scams include those surrounding the tax season.

How can I identify malicious e-mail?

Oftentimes there are key identifiers you can use to recognize suspicious e-mail.

1. **Identify the Sender.** Do you know this person? Were you expecting e-mail from this person or does it fit in with your job role? If not, it is probably suspicious. If you know the person, check with them using a communication method you have outside the email in question. (e.g., call the individual using a phone number you know to be valid)
2. **Reply-to.** If the Reply-to address is different from the sending address, this should raise your suspicion for the whole message.
3. **Links and Attachments.** If you were not expecting an attachment or a link, and you do not know the sender, do not open it! If you are not sure, check with the sender by phone (don't use a phone number in the e-mail), otherwise report it.
4. **Grammar and Tone.** Many of the malicious e-mails sent have poor grammar, punctuation and spelling. In addition, you should know how your co-workers communicate. Does this message sound like them? If not, it is probably malicious.
5. **Emotions.** Be wary of any e-mails trying to cause certain emotions. The most commonly-used malicious emotions are:
    - **Greed.** Messages offering or promising you money by clicking a link or giving away information are usually malicious. If it seems too good to be true, it probably is.
    - **Urgency.** Unusually short deadlines create a false sense of urgency to act. Attackers employ this technique in attempts to confuse the recipient.
    - **Curiosity.** Attackers take advantage of our curiosity by promising something exciting or prohibited content.
    - **Fear.** Threatening recipients with negative consequences is a common tactic to generate responses—things such as threatening to shut off accounts or legal action.

How can I report suspicious e-mail?

All URMC and Affiliates workforce members who receive suspicious e-mail should report it immediately to abuse@rochester.edu or abuse@urmc.rochester.edu. Even if you are not sure, it is better to have the message checked first. In addition, just because you may think it is obviously bad, you should still send it along for analysis. What might be obvious to you may not be to another individual. Remember, **if you see something suspicious, report it!**

How can I make sure my message looks legitimate?

Several actions will help make your messages look legitimate.

1. **Use links to sites with "https://"** This directs your recipients to websites that can be verified by a trusted third party.
2. **Offer alternatives to clicking the link.** Give directions such as "Go to the Intranet, click on …"
3. **Have direct contact information.** Give your recipients a point of contact to verify the authenticity of the message.
4. **Avoid attachments.** Where possible avoid sending attachments. Try to use departmental file shares or other methods of file transfer.

For any questions on this topic or any others regarding HIPAA, please contact your Privacy Officer or HIPAA Security Official.