State of Illinois
Department of Innovation & Technology

SOCIAL ENGINEERING: TRICK OR TREAT OR SHOULD WE SAY TRICK OR THREAT?

Cyber Bulletin 4

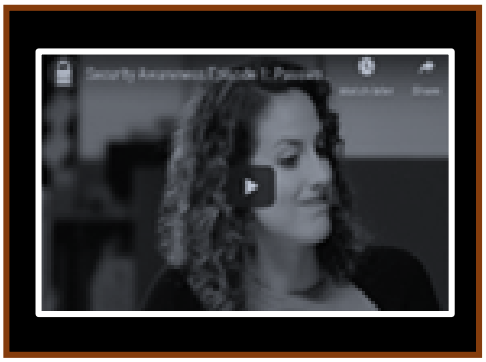
Trick or Threat! What can you do to help ensure cyber safety?

This is our last week of Cybersecurity month and the focus is social engineering. Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. We commonly refer to all types of social engineering as "Phishing". These phishing attempts come by email, text, calls, and websites. 2020 has certainly provided criminals with a lot of new opportunities to try and get us to click on links or open attachments.

Here are FOUR popular phishing scams from the past month:

1. **TEXT:** Unclaimed Assets Notice: Our records show XXX in funds owed to you. Verify HERE
   What to do: Delete it.
2. **TEXT:** Important notification regarding your USPS delivery…Proceed to XXXXXX.
   What to do: Delete it. If you are worried about a true delivery, go to the site of where you might have ordered something.
3. **EMAIL:** Amazon delivery notice…please click here to see the status of your delivery.
   What to do: Delete it and simply go to your Amazon account quick link to check your order status.
4. **EMAIL:** Any major website you do business with: Unusual Account Activity and login from a different device.
   What to do: Some of these emails or text look legitimate. Solve this question of legitimacy by simply going to and resetting the password. No need to click "HERE". While in your account, set up MFA!

Spooky Cybersecurity Videos



Click here to view more cybersecurity videos

Need to report a security issue?

The Department of Innovation & Technology (DoIT) is committed to protecting our customers. If you have found a vulnerability or security issue, we ask that you submit a detailed description of the issue to us at: DoIT.Security@illinois.gov.