Identifying and Avoiding Social Engineering Attacks While Working from Home

With so many higher education faculty and staff working from home—many for the first time—malicious hackers and identity thieves will be probing for ways to access sensitive data.

Here are a few things to keep in mind to protect yourself, your students and your institution while working from home.

Know the **Risks**

They are called "social engineering" attacks because they use your social connections to bypass your internal threat detectors and do what the hackers want you to do.

Hackers will often impersonate school executives and administrators, institutional organizations, or even students to trigger the response they're looking for.

Attackers may harvest information from highly public institutional organization charts, academic programs, and even individual instructors and courses for greater credibility.

Knowing these attacks are coming and remaining vigilant against unusual requests is critical to reducing the risk of malware, ransomware, data breaches, and compromising your credentials.

Know How **Attacks Happen**

Attackers use email, mobile device text/messaging, and social media accounts to engage victims:

TEXT

Attackers send messages directly to your mobile device, too, requesting action via clicking links, downloading files, or opening attachments. Slow down and double-check sender and content before replying or engaging text messages. When in doubt, call them to confirm!

PHONE CALLS

With everyone working remotely, the chances of phone call attacks is on the rise. If someone contacts you claiming to be from the IT department, an internal department or a technology vendor and asks you for sensitive information, **do not provide it without confirming first!** Get an email address or ask them a question about your institution that only employees would know.

EMAIL

Social engineering emails can be very convincing! Slow down before you respond and watch for unusual contacts, odd urgency in the message, suggestions you failed to do something important, or a threating or angry tone. All are signs that you may be under attack.

Remember **Key Security Behaviors**

01

Never give up your login information or passwords to anyone, ever! Nobody with real authority (like your IT team or Microsoft) needs this information.

02

Enable multifactor authentication (MFA) on all logins if the option exists. A common MFA method is to key in a code sent to your phone along with your password. This way, even if hackers get access to your credentials, they still can't log in.

03

Do not click links or downloads without double-checking sender and content first, and never open attachments you are not expecting.

04

Verify before acting... using a different channel. If you get a suspicious email, don't respond to it. Call the person to confirm before sharing any sensitive information or files.

05

Hover over—but don't click!—on any links. Does the URL look legitimate? Are all the links pointing to different URLs? If not, you've discovered a phishing attack. Delete or report it to your IT team.

06

Never use or scan USB storage devices unless absolutely certain of their origin.

Thank you for following these steps to ensure the security of our institution's systems and data.

Dynamic Campus

Info@DynamicCampus.com | (888) 805-3022 | www.DynamicCampus.com