Dynamic Campus

Cybersecurity Tips for Higher Education While Working from Home

As more higher education faculty and staff work from home—many for the first time—here are some quick tips everyone should follow to protect yourself, your students and your institution:

One-Time **Security Measures**

01

Make sure your laptops, phones, tablets and other devices require a password, fingerprint or facial recognition in order to unlock them.

02

Enable multifactor authentication (MFA)—using a code sent to your phone in addition to using a password, for example—whenever possible.

03

If you're using a personal device for work, be sure to install, use and automatically update antivirus software and tools, some of which are included with Windows 10.

04

Enable your antivirus protection to perform regular malware scans, ideally daily. They can often run in the background and cause no interruption.

05

Optimize the web-filtering security settings on your browser by searching for "[browser name] security settings" and follow the recommended guidelines.

06

Secure your WiFi network and hide the network to prevent it from being identified by strangers, and change the default hardware password.

Connection **Security**

07

If your institution provides virtual private network (VPN) access, always connect using the VPN when conducting institutional business.

08

Disconnect from the VPN before conducting personal tasks like searches, email, social media, etc. to secure institutional systems and data.

09

Do not send sensitive information like personal or financial data over standard email, which is as secure as sendinga postcard in the mail. Turn on your email program's Encrypt options (or Message Encryption) or use secure cloud storage for sending sensitive information.

10

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

Stay **Vigilant**

With everyone working apart, its easier for hackers to trick you into giving up sensitive information by acting like a trusted brand, authority, or co-worker.

11

These attacks can happen anywhere, any time, including by email, attachment, text, call or even social media.

12

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

13

Check the sender. Is the source or sender's email address legitimate? If it doesn't line up, delete it or report it to your IT team.

14

Before clicking a link, just hover your mouse over it. 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.

15

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.

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

Dynamic Campus

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

www.DynamicCampus.com