NKU | OFFICE OF Information Technology

Cybersecurity Tips for NKU
While Working from Home

As faculty and staff work from home—many for the first time—here are some quick tips everyone should follow to protect yourself, our students and NKU.

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

03

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

04

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.

05

Secure your WiFi network and change the default hardware password.

Connection Security

06

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

07

Use only known USB storage devices and be absolutely certain of their origin!

Stay Vigilant

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

08

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

09

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

10 Carefully check the sender. Is the sender's email address legitimate? Spoofing occurs that is close, but not quite right. If it doesn't line up, Report it to Abuse@nku.edu.

11

Before clicking a link, hover your mouse over it.. Make sure the URL says https:// xxxx. safelinks. xxxx (or safeattachment) . If not, you've discovered a phishing attack. Report it to your IT team at Abuse@nku.edu.

12

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 NKU's systems and data!