

Dear Campus Community,

Since the onset of the coronavirus there has been a noticeable increase in cyberattacks worldwide. Both the volume and sophistication of the attacks are being reported by agencies tracking this activity. The Millersville IT Network team has noticed a similar pattern of activity attempting to intrude the MU network.

What the MU Network team is reporting:

- A dramatic increase in phishing scams and ransomware campaigns. These 'bad actors' are fraudulently using "COVID-19" to solicit activity that provides access to computers and networks aimed at stealing personal information such as passwords, ID details, bank account details, credit card numbers, etc.
- A 20% increase from foreign countries attempting to intrude the MU network.

Millersville has a robust Intrusion Prevention System in place to isolate such attempts.

What can you do to maintain security for the Millersville infrastructure and your personal devices:

- Report suspicious activity
 - Attackers and scammers have been known to exploit heightened emotions and panic.
 - Avoid the "last minute" requests that are appearing. STOP, THINK!!!
 - Please, if you feel as though something is "out of the norm" with the email or notification, either report the email as spam, or forward the correspondence to the helpdesk at help.desk@millersville.edu.
 - REMEMBER: You can always reach out to verify if a request is correct/real. That one extra step can alleviate any misgivings.
- Refrain from using non-Millersville email systems (google, hotmail, etc.) for University business.
- Avoid using public Wi-Fi wherever possible
- If Using a personal device to conduct University business:
 - Ensure anti-virus software is up-to-date
 - Ensure operating systems are up-to-date

As always, the IT department staff remains available to support your technical needs. Please check <https://wiki.millersville.edu/display/ittac/welcome> for help desk contact information and additional technical topics.

Thank you,
Stephen J. diFilipo, Jr.
Chief Technology Officer