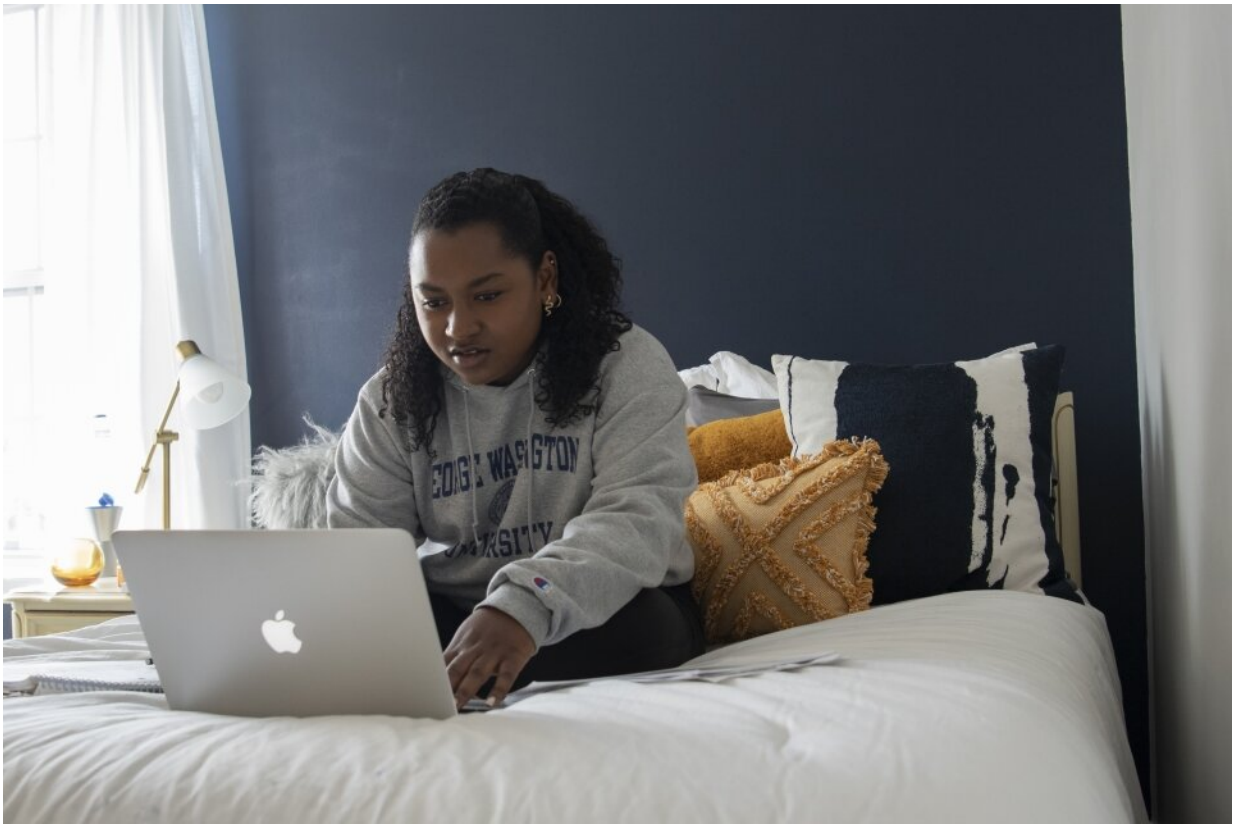
Concerns about cybersecurity increase during COVID-19

May 21 2020, by Tatyana Hopkins



Cybersecurity becomes an increased concern for GW students, faculty and staff working through the virtual learning period. Credit: Sydney Elle Gray/GW Today

Cyber criminals are taking advantage of the COVID-19 crisis, as

cybersecurity experts have tracked a rise in online scams related to the novel coronavirus. Using concerns about the novel coronavirus, cyber criminals have launched deceptive phishing and websites related to the pandemic.

The FBI has issued alerts regarding scams related to fake donations, coronavirus cures and expedited stimulus checks. Google announced that it blocked 18 million daily malware and phishing emails related to COVID-19, in addition to more than 240 million COVID-related spam messages. The Federal Trade Commission has reported that coronavirus-related scams have cost Americans more than $33 million so far this year.

Diana Burley, a professor in the George Washington University Graduate School of Education and Human Development, a cybersecurity expert and executive director and chair of the GW Institute for Information Infrastructure (I3P), spoke with GW Today about how to stay protected against online scams:

Q: How have online scams used misinformation and specific vulnerabilities associated with the COVID-19 crisis?

A: Bad actors are actively working to take advantage of the uncertainty and shortage of reliable information about topics of urgent interest—coronavirus facts, stimulus payments and even opportunities for charitable giving.

They are creating fake websites, sharing misinformation through social media and using social engineering schemes such as email phishing attacks to trick users into revealing private information. All of these methods are designed to exploit the heightened anxiety of the crisis.

As the nation begins to emerge from quarantine, we need to watch for new schemes designed to take advantage of vulnerabilities associated with the reopening phase.

Q: How can internet users verify the information they come across related to the pandemic?

A: Users should be careful of information shared on social media, even if the information came from a friend, and whenever possible they should verify the original source before accepting the information as valid. They should be wary of newly-created entities claiming to have unique, unrecognized or unknown sources of information.

There are several good options to verify COVID-19 related information. Both the federal government and state and local jurisdictions, like Washington D.C., have established information sites to provide citizens with up-to-date crisis-related information.

Most employers are providing updates and information on appropriate procedures for their teleworking employees. Similarly, established retailers and service providers also offer guidance to successfully engage in online services.

Q: Are there any groups that are particularly vulnerable to emerging online scams?

A: Everyone is vulnerable, and we all need to be vigilant.

In this tumultuous environment—where information is constantly evolving, individual circumstances are changing frequently and where people are scared— everyone, even the most seasoned online users, can fall victim to scammers.

For example, an individual may be a regular online shopper but unfamiliar with telemedicine, another may be completely new to online shopping, and someone else may be accustomed to accessing the internet largely through more secure workplace systems and thus may operate with a false sense of security at home. Each of these individuals represent groups who are vulnerable for different reasons.

It is not an overstatement to say that we must all be mindful of our online habits. Bad actors are looking to exploit any vulnerability available to them. For all of us, both security and privacy concerns must remain top of mind as we continue to leverage digital platforms to work, shop, learn and stay socially connected.

Q: What recommendations or tips do you have for internet users to maintain security online?

A: Internet users can follow several fairly simple and inexpensive methods to protect themselves online. While not an exhaustive list, the following recommendations will enhance user security in cyberspace:

- Practice cybersecurity best practices. Use strong passwords and vary them across different websites. Never send credentials via email, back up your data and practice safe browsing habits.
- Stay updated. Keep anti-virus software and applications up to date. Remember that software companies use updates to provide both functionality and security upgrades that address new vulnerabilities. This is also true for your cell phone.
- Use two-factor authentication. Using multiple methods to verify your identity, provides added protection. If, for example, your password has been compromised, using two-factor authentication that requires both a password and a verification code sent to your cellphone to login, will help to safeguard your accounts.

- Trust, but verify. If you receive a message and are unsure about the sender or request, verify its legitimacy before taking other action. For instance, if the message is purported to be from your doctor or supervisor, call the office and confirm the authenticity of the request. Never click on a link if you are unsure of the sender.
- Seek help. If you are teleworking and have a question, follow the guidance of your IT department. If you are using your personal devices, reach out to your service providers.

The Cybersecurity and Infrastructure Security Agency provides advice for business owners and individual citizens on how to stay safe online. University experts, professors and institutes like I3P can also provide advice on how to navigate the evolving internet landscape.

Provided by George Washington University