October 16, 2018

Cyber: It's Everyone's Job to Ensure Online Safety at Work

In honor of National Cybersecurity Awareness Month, the DC Homeland Security and Emergency Management Agency (HSEMA) is sharing important tips each week in October to help digital users within the District learn more about cybersecurity and how to better protect themselves and their loved ones from cyber threats.

In the workplace, we all have a shared responsibility to help protect our organizations from hacks, data breaches, and other cyber threats. Although the word "cybersecurity" may not be included in our official job descriptions, there are several easy ways we can help reduce the risk of a successful and devastating cyber attack conducted against our employers. The following tips can help you to become a more cybersecurity-conscious employee.

- **Passwords**: Don't make passwords visible to others in your office, such as on whiteboards or sticky notes. Make sure the passwords you use for work accounts are lengthy and secure, using a combination of upper and lowercase letters, numbers, and symbols. Avoid reusing the same password for different accounts.

- **Two-Factor Authentication (2FA)**: Enable 2FA on every work account that offers it. This security feature can help prevent unauthorized access to your accounts if your password is stolen.

- **Wi-Fi Hotspots**: Don't use work-issued devices such as laptops and cell phones to connect to public Wi-Fi hotspots. Some hotspots can be malicious and hackers may be able to see information you send over the network. If you absolutely must use a public Wi-Fi hotspot, be sure to use a virtual private network, or VPN, to encrypt your network traffic and secure it from prying eyes.

- **USB flash drives**: Never insert an unknown or untrusted USB flash drive into your work computer, including those provided at conferences. Hackers have been known to drop malware-laden USB flash drives in parking lots to entice curious employees into plugging them into their work computers, thus bypassing network perimeter defenses.

- **Phishing:** Your organization may have email filtering software in place, but a phishing email may still slip through the filter to your inbox from time to time. It's important to recognize unexpected or unfamiliar emails and avoid clicking on any links or opening attachments in them. Notify your organization's IT department immediately if you believe you have received a phishing email.

For more cybersecurity tips, visit the District of Columbia's Office of the Chief Technology Officer (OCTO) at octo.dc.gov/cybersecurity and the National Cyber Security Alliance at StaySafeOnline.org.