FROM THE DESK OF MILIND SAMANT, ISO

In its most recent annual Cost of a Data Breach report, the Ponemon Institute reviewed more than 500 incidents around the world. The results were sobering: the average data breach costs an organization $4.24 million, and takes 287 days to identify and contain. That's why Cybersecurity Awareness Month – designated every October for the last 18 years – is an important reminder of just how critical cybersecurity awareness is at all levels. The best way to protect our College and ourselves is by being able to recognize potential cyber threats, understand their significance, and sharing that knowledge with others. The weakest link in many cybersecurity programs is people. They make mistakes, it's bound to happen. But if we can raise our awareness about cybersecurity across all of the platforms and devices we use, it can drastically reduce the likelihood of a mistake happening. Even more important – when a mistake does happen and we have a strong cybersecurity posture, people recognize it and know how to respond.

This past October, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance (NCSA) are emphasizing the overarching theme of "Do your part. #BeCyberSmart."

SECURING INTERNET *Connected Devices*

Internet-connected devices are helping homeowners increase efficiency, reduce costs, conserve energy and a whole host of other benefits. However, with all of these benefits come risks to privacy and security. Understanding the basic security practices to keep your family and these devices safe are extremely important. Please follow the tips and links below for more details on this security risk.

DO YOUR HOMEWORK

- Before purchasing a new smart device, do your research on it
- Check out user reviews and see if there have been any security/ privacy concerns reported
- Understand what security features the device has, or doesn't have
- Purchasing from a reputable company is of utmost importance for privacy and security concerns
- The functionality of most Internet of Things (IoT) devices requires collecting data
- Take the time to understand what information your connected devices collect, how that information is used, and if shared with third parties
- Understand where your data will reside (e.g. cloud) and the security protecting your personal information
- The moment you turn on a new "smart" device, configure its privacy and security settings

CHANGE DEFAULT USERNAMES AND PASSWORDS

- Many IoT devices come with default passwords and this is a top way these devices get attacked and become compromised
- Change the default setting and configurations of the device
- Create long and unique passphrases for all accounts and use multi-factor authentication (MFA) wherever possible
- Fortify your online accounts with MFA by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device

KEEP SOFTWARE UP TO DATE AND DISABLE FEATURES

- Devices with critical security patches can be compromised and vulnerable to attack
- When the manufacturer issues a software or firmware update, patch it immediately
- Updates include important changes that improve the performance and security of your devices
- Disable features on the device you will never need or will never want to use
- Don't ignore but keep your phone software and associated IoT apps up to date

PAY ATTENTION TO THE WI-FI ROUTER IN YOUR HOME

- Use a strong password to protect your router
- Name the router in a way that won't let people know it's your house
- Keep the router software up to date by checking with the manufacturer or Internet Service Provider (ISP) to see if the software is updated automatically

LINKS AND RESOURCES FOR FURTHER INFORMATION

- NIST: What is the Internet of Things (IoT) and How Can We Secure It?
- CISA: Securing the Internet of Things

Learn more about National Cyber Security Awareness Month.
National Cyber Security Awareness Month.

REMINDERS:
Set a strong password: Use at least 8 characters in upper and lower case, numbers, and symbols;
Keep your device locked: Use a password, pin, pattern, or fingerprint lock when you are not actively using it.
When in doubt, throw it out and contact the *Service Desk at servicedesk@oldwestbury.edu* or call X3098.

ITS INFORMATION TECHNOLOGY SERVICES

The information provided in the email message is intended to increase the data security awareness of SUNY Old Westbury end users and to help them behave in a more secure manner within SUNY Old Westbury work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the SUNY Old Westbury's overall cyber security posture.

Disclaimer: These links are provided because they have information that may be useful. The SUNY Old Westbury ITS Department does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein.