Best Practices in the Workplace and While Working Remotely

GEORGIA TECHNOLOGY AUTHORITY

NCSAM 2023

Protecting Your Org!

Everyone in an organization is susceptible to becoming a victim of cybercrime. It is important to educate employees on best practices that reduce the risk of a data breach or cyber-attack. With proper cybersecurity awareness training, each employee should be equipped with knowledge that will allow safe internet use in and out of the office.

Creating strong passwords, completing awareness training, implementing an incident response plan, and creating organizational policies are all simple tasks that can be done to reduce the risk of cybercrime. Cybersecurity is everyone's responsibility; we must do our best to protect our organization and its employees!

Although simple tasks like locking your computer seems small, they have a huge impact on your org's security. Security starts with you!

"If you think technology can solve your security problems, then you don't understand the problems, and you don't understand the technology."

Fun Facts!

1. Every 39 seconds there is a cyber-attack.

2. A hacker can attempt 2.18 trillion combinations of passwords and usernames in 22 seconds.

3. More than 1 billion malware programs exist.

4. One single security breach can lead to exposing the personal information of millions of people.

5. Data breaches in the U.S. cost twice as much as the global average.

6. Phishing attacks increased by 48% in the first half of 2022, with reports of 11,395 incidents costing businesses a total of $12.3 million.

Tips for Online Safety at Work!

In Office

1. Think before you click! Most cyber-attacks occur from phishing emails.
2. Complete cyber awareness training.
3. Use multi-factor authentication.
4. Secure devices by locking them when you are away from your desk.
5. Report security incidents.
6. Use strong passwords.
7. Always make sure you have the latest software and app updates.
8. Never download apps that look suspicious or come from an unknown source.

Telework

1. Know your organization's telework policies.
2. Avoid unsecure Wi-Fi and use a VPN
3. Only use organizational approved devices.
4. Guard passwords and other sensitive information in public.
5. Secure your home router.
6. Use a secure file-sharing solution to encrypt data when sharing confidential information.

Lock it down, protect it up, and block the hackers!