Online Safety at Home

GEORGIA TECHNOLOGY AUTHORITY

NCSAM 2023

What Do You Do Online?

Online safety, also known as internet safety or cyber safety, refers to the practice of protecting yourself, your personal information, and your digital devices while navigating the vast and interconnected world of the internet.

With the increasing reliance on the internet for communication, work, school, shopping, and more, understanding and implementing online safety measures has become essential. This includes safeguarding against threats such as identity theft, malware, phishing, and other online risks.

In an age where our digital footprint is extensive, staying informed about online safety best practices is crucial to enjoy the benefits of the internet while minimizing potential harm or exposure to cyber threats.

No matter the reason for your internet use, threat actors have capabilities to attack from every front. So, ask yourself “What do I do online” and take the necessary steps to protect yourself.

“Hacking just means building something quickly or testing the boundaries of what can be done.”

Fun Facts!

1. “123456” and “password” were among the most used passwords.

2. Human error accounts for 95% of cyber-attacks.

3. On average people forget their passwords about 37 times a year.

4. Email scams are among the most financially damaging Online Crime.

5. The world’s longest password on record was over 1,300 characters long.

6. World Password Day is celebrated on the first Thursday of May each year.

7. Phishing remains the #1 types of cybercrime

Tips for Online Safety!

Work

1. Use strong, unique complex passwords.
2. Beware of Phishing.
3. Participate in employee training.
4. Secure devices by locking them when not in use.
5. Report security incidents.
6. Use passwords and waiting rooms for video conferences to control access.

Shopping

1. Only shop from reputable websites.
2. Enable two-factor authentication.
3. Check website security before entering payment information.
4. Never leave your cards connected to apps when not in use.
5. Avoid making purchases when connected to public wi-fi.

Kids

1. Set age-appropriate boundaries for websites and apps.
2. Don't respond to unknown or unexpected communications.
3. Maintain open communication about online activities.
4. Educate about the importance of not sharing personal information online.
5. Pay close attention to who your child engages with online.
6. Educate your child on cyberbullying
7. Encourage children to report inappropriate behavior.

Home

1. Always change default router login credentials.
2. Update software.
3. Regularly back up data.
4. Limit personal information sharing.
5. Set up a Virtual Private Network (VPN).

Stay Secure, Search with Care

Online Security Everywhere!