CAMPUSGUARD®

A Merchant Preservation Services Company

CHAMPION
National Cyber Security Awareness Month

CyberSecurity Checklist

Best practices that can significantly reduce the risk of you becoming a victim of a security breach...

Update Operating Systems and Anti-Virus Software
Ensure your operating system is set for automatic updates, and reboot your system regularly. Anti-virus and anti-malware programs should automatically check for updates and scan your devices.

Use Strong Passwords
Use complex passwords or passphrases, at least 8 characters with a combination of upper and lower case letters, numbers, and special characters. Change your password at least every 90 days and don't reuse passwords across multiple systems. Do not share your password with others.

Need to Know Access
Only those individuals with a specific need to know should be authorized to access sensitive information. Least privilege necessary is a good practice to stick with.

Maintain an Accurate Inventory
Know where sensitive information resides and keep track of servers, workstations, mobile devices, back-up systems, etc.

Secure Devices
Any device that holds sensitive information should be locked when not in use and encrypted. Don't misplace devices or leave them vulnerable to theft.

Secure Information Disposal
All paper documents with sensitive information should be shredded. Electronic media must be thoroughly reformatted or physically destroyed.

Back up Data
Can you retrieve back up files of data or copies of critical information?

Secure Transmission
Do not send sensitive information via unencrypted e-mail or other unsecured messaging methods.

E-mail Awareness
Be skeptical of e-mails and do not click on or open suspicious attachments or links.

Connect Securely
Only connect to trusted, private networks. Do not connect to public Wi-fi networks.