CYBER GUIDELINES AND TIPS FOR SMALL BUSINESSES

From the Stop.Think.Connect. campaign from the Cybersecurity & Infrastructure Security Agency

REGULARLY BACKUP ALL DATA

Backup critical data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.

KEEP CLEAN MACHINES

Keep your anti-virus and anti-malware up to date. Having the latest security software, web browser, and operating system is the best defense against viruses.

CREATE MOBILE DEVICE ACTION PLAN

Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks

EDUCATE EMPLOYEES

Ensure they are knowledgeable about threats and how to deal with them. Require them to follow security policies and have clear consequences for violating such policies.

SECURE WIFI NETWORKS

Wi-Fi network should be secure, encrypted, and hidden. Password protect access to the router.

CONTROL PHYSICAL ACCESS

Prevent access or use of business computers by unauthorized individuals. Make sure a separate user account is created for each employee.

PROVIDE FIREWALL PROTECTION

Make sure the operating system's firewall is enabled or install free firewall software available online.

PASSWORDS AND AUTHENTICATION

Require unique passwords and change passwords every three months. Implement multi factor authentication that requires additional information beyond a password to gain entry.

LIMIT EMPLOYEE ACCESS TO DATA

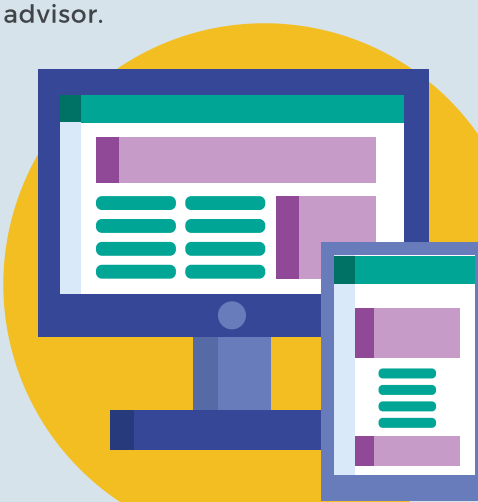
Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

EMPLOY BEST PRACTICES FOR PAYMENT CARDS

Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. Isolate payment systems from other, less secure programs.

FIND OUT IF YOUR SBDC HAS A CYBER ADVISOR

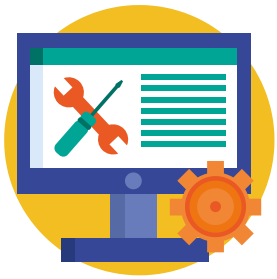
Reach out to your SBDC for one-on-one guidance and counseling with a cyber advisor.



FUNDAMENTALS FOR CYBER HYGIENE

- All businesses collect some form of sensitive, valuable information.
- Cyber incidents will occur.
- Data stewardship, privacy and incident readiness are everyone's responsibility.
- Data management and privacy practices need continual review.
- Every organization needs to have a current, tested response plan.
- Ongoing employee training is a critical key to success.

*OTA's 2018 Cyber Incident and Breach Trends Report



RESOURCES

One-on-one counseling with a SBDC Cyber Advisor.
www.fcc.gov/cyberplanner (Cyber Planner)
www.us-cert.gov-ccubedvp (Self-Assessment Tool)
Nist.gov/itl/smallbusinesscyber (Small Business Corner)
Cisa.gov/cyber-essentials (Small BusinessToolkit)
www.eset.com/us/cybertraining (Additional free trainings)
Wizer-training.com (EmployeeTraining Videos)
Ftc.gov/Smallbusiness (Videos, Tools and Quizzes)
Fico.com/en/products/cyber-risk-score (Get Your Cyber Risk Score)

"THE DESIGN AND DEVELOPMENT OF THIS TIP SHEET WAS FUNDED BY THE U.S. DEPARTMENT OF DEFENSE OFFICE OF LOCAL DEFENSE COMMUNITY COOPERATION (OLDCC) CASCADE GRANT THROUGH THE CALIFORNIA GOVERNOR'S OFFICE OF PLANNING AND RESEARCH.
. THE CONTENT WAS DRAFTED BY ECEDC IN COLLABORATION WITH STATEWIDE CASCADE PARTNERS AND DOES NOT NECESSARILY REFLECT THE VIEWS OF OLDCC AND OPR."