The Arkansas Cyber Defense Center

Top 10 Cyber Best Practices

1. Use strong passwords, or auto generated passwords.
The best password manager software will alert you if your existing passwords are weak, reused, or have been tagged in a data breach. These products help you improve your password hygiene by suggesting new, strong, and unique credentials for every login.

2. Implement multi-factor authentication on your accounts.
Multi-factor authentication can help you become 99% less likely to get hacked. Enable multi-factor authentication on your email, social media, online shopping, financial services accounts, and anywhere else sensitive data or systems are. Don't forget your gaming and streaming entertainment services. Deploy additional Data Loss Prevention capabilities when possible.

3. Think before you click, and be careful what you download.
Emails are a common way for malicious activity to enter an organization's network. Beware email phishing links! Always hover over a link that is unfamiliar to see where it is linked to. Never click-on or download data that seems uncommon in the workplace.

4. Use trusted antivirus/antimalware software.
Confirm the organization's devices and networks are protected by antivirus/antimalware software and signatures in the tools are updated.

5. Keep all devices patched, up-to-date, and within support lifecycles. Be sure that all computers, phones, tablets, and other devices are regularly updated. Check the manufacturer's support lifecycles and decide when it's time to upgrade.

6. Never leave devices unattended.
If you need to leave your laptop, phone, or tablet for any length of time, lock it up so no one else can use it. If you keep protected data on a flash drive or external hard drive, make sure it's encrypted and locked up as well. For desktop computers, lock your screen or shutdown the system when not in use.

7. Train employees and have an actionable Cyber Plan.
Establish security practices and policies to protect sensitive information. Educate employees about cyber threats and how to protect your organization's data. Hold employees accountable to the Internet security policies and procedures. Your Cyber Plan should provide specific, concrete procedures to follow in the event of a cyber incident.

8. Identify the most important (vulnerable) network assets.
Prioritizing the protection of an organization's "crown jewels" and assessing how to manage the risk associated with protecting them are important first steps toward preventing the type of catastrophic harm that can result from a cyber incident.

9. Regularly perform data backups.
Test backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyber attack; ensure that backups are isolated from network connections.

10. Always use secure, trusted connections.
Any network other than your home or work network is likely an insecure network (ex. public Wi-Fi such as hotels airports and other free networks). Make sure the lock pad is present beside the address bar when browsing the Internet. Be sure to keep firewalls, routers and Wi-Fi access points up-to-date as well.

* Refer to your insurance carrier, cyber advisor, attorney or managed service provider for more specific expert opinions and recommendations.

POWERED BY SBA
U.S. Small Business Administration

REPORT A CYBER INCIDENT:

forge.institute/acdc
501-239-9599