DATA ASSURED

Cyber Tips

In Partnership with:

AMERICA'S SBDC DELAWARE

AMERICA'S SBDC KENTUCKY

1 Protect endpoint devices against unseen threats

- Prepare devices for unknown threats by equipping them with monitoring tools such as Watchdog by Anchor Security to provide anomaly detection, vulnerability analysis, and active response to block out new threats

2 Implement Scheduled backup with version control

- In the event that systems are unable to prevent data loss, or needing an older version of a file, having version-controlled backup for all important files will put your mind at rest knowing that you can get any of your files back at any stage from their life.
- Ensure that access to this data is controlled based on user roles, so that data is only accessible by required personel

3 Create strong security usage policies to protect your customers and your employees

- The best way to prevent hackers access is to practice device and service usage in ways that block them out entirely. Enforcing multi factor authentication, string passwords, encryption where ever possible, and a strong common sense when checking email can go farther than you may expect
- Clearly define consequences for violating such policies
- Hold your employees accountable for any sensitive data they handle or interact with
- Require strong passwords and enforce frequent and significant changes

www.KentuckySBDC.com

4 Control physical access to devices

- Ensuring physical security is essential. Hackers who are able to gain physical access are far more dangerous than remote
- Requiring biometric authentication can take the ease out of dealing with long and tedious passwords, thus increasing security

5 Encrypt all connections, no matter the need

- Not only will this inspire confidence from your customers and clients, but it can prevent many unforeseen issues down the road
- Show the public that security is a priority for your company and its digital footprint

6 Educate employees

- Ensure they are knowledgeable about threats, and how to deal with them
- Make sure they are able to follow security usage policies by having the knowledge to perform all required actions securely.

7 Secure Networks

- Your network is often the first thing that hackers see, and your first line of defense. Make sure it can handle what ever is thrown its way
- Implement an IDS to detect malicious and anomalous network usage
- Ensure that any guest networks are inoperable with corporate networks
- Use MAC address whitelisting and IP filtering to make sure only the devices you trust are on the network, and can talk to only the other devices they need to
- Isolate payment systems to their own network so that any compromise does not mean the loss of both corporate systems and payment systems

The Kentucky Small Business Development Center is funded in part through a cooperative agreement with the U.S. Small Business Administration and supported by a consortium of the public and private sector. Headquartered at the University of Kentucky, the Kentucky SBDC is working in partnership with other institutions of higher education and economic development agencies to provide business coaching and continuing education opportunities to Kentucky's entrepreneurs.