DATA ASSURED

Cyber Tips

UNIVERSITY OF DELAWARE
ECONOMIC INNOVATION
& PARTNERSHIPS

AMERICA'S SBDC DELAWARE
Small Business
Development
Center

1 Protect 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 backups with version control

- If security systems are unable to prevent data loss, or you require an older version of a file, having version-controlled backups for all important files is a must. Knowing that you can get any of your files back at any stage in time will put your mind at rest
- Ensure that access to this data is controlled based on user roles, so that data is only accessible by required personnel

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

- The best way to prevent unauthorized access is to practice device and service usage in ways that block them out entirely. Using multi-factor authentication, passphrases, encryption wherever 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

AMERICA'S
SBDC®
DELAWARE
www.DelawareSBDC.org

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 hackers
- Requiring biometric authentication eases the burden of using 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 secure 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 whatever is thrown its way
- Implement an Intrusion Detection Software to detect malicious and anomalous network usage
- Ensure that any guest networks are completely separated from 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 on their own network so that a breach won't not mean the loss of both corporate data and payment data

The Delaware SBDC, a unit of the University of Delaware's Office of Economic Innovation and Partnerships (OEIP), is funded in part through a cooperative agreement with the U.S. Small Business Administration (SBA) and the State of Delaware.