DATA ASSURED

Cyber Tips

In Partnership With:

AMERICA'S SBDC DELAWARE | PHIN SECURITY

Presented By:

AMERICA'S SBDC CONNECTICUT | Small Business Development Center

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 personnel

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.ctsbdc.uconn.edu

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

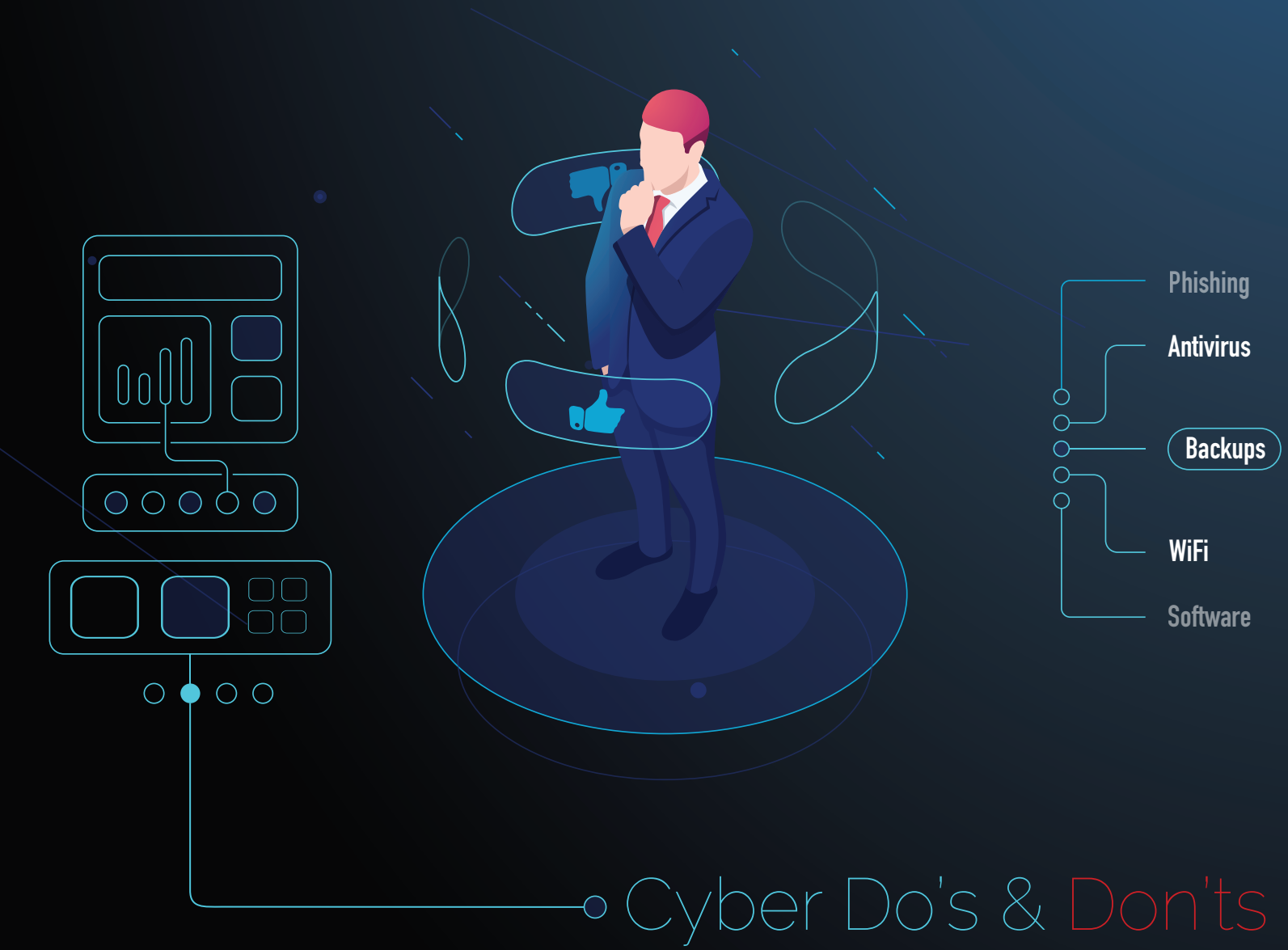
6 Educate employees

- 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

DATA ASSURED



Cyber Do's & Don'ts

In Partnership With:

AMERICA'S SBDC DELAWARE | Small Business Development Center

Presented By:

AMERICA'S SBDC CONNECTICUT | Small Business Development Center

DO'S:	DON'TS:
Use unique complex passphrases and change them regularly	Open attachments or click links from unknown sources
Turn on encryption on all devices	Use free public WiFi without a VPN
Regularly backup all your data with version controlled backups	Share passphrases or use the same phrase for multiple accounts
Use antivirus/antimalware on all devices	Scan random QR codes or accept random Airdrops
Keep all software and OS's up to date	Install apps or software from unknown sources
Pay attention to possible signs of phishing	Recycle old devices without properly wiping all data
Educate all employees	Log into any personal accounts on public computers
Create a data breach response plan	Leave unused services running on your devices. *Ex. Bluetooth*
Use multi-factor authentication when possible	Plug in random portable devices
Get a cybersecurity insurance policy	Visit insecure websites (Sites without the "S" in HTTPS)

CTSBDC@uconn.edu

www.ctsbdc.uconn.edu

(877) 723-2828

DATA ASSURED

Cyber Solutions

In Partnership With:

America's SBDC Delaware | PHIN SECURITY

Presented By:

America's SBDC Connecticut | Small Business Development Center

Encryption:

- FileVault (macOS)
- BitLocker (Windows)
- VeraCrypt
- AxCrypt

Digital Infrastructure:

- Google Cloud
- Amazon S3
- DigitalOcean Spaces
- Microsoft Azure

Cloud File Storage:

- Google Drive
- Microsoft OneDrive/SharePoint
- Dropbox
- iDrive

We understand that cybersecurity is a new and scary area for a lot of small businesses. This is usually because as a small business owner you just do not know where to start. This is why we created this cyber solutions one-pager, to help give every business owner a starting point. These listings are provided solely as convenience. Connecticut SBDC does not imply or intend endorsement nor accept any responsibility for the use of products and/or services provided by listed companies. Nor does the Connecticut SBDC warrant the quality, safety, suitability, or reliability of listed companies, their products and/or services.)

File backup:

- EaseUS
- Paragon Backup & Recovery
- File History (Windows)
- Time Machine (macOS)

Virtual Private Network (VPN):

- ExpressVPN
- Private Internet Access
- CyberGhost VPN
- Surfshark

Password Management:

- Lastpass
- 1Password
- Dashlane
- Keeper

Threat Detection Services:

- Trustwave
- WatchGuard
- Digital Guardian
- Symantec Security

Desktop as a Service (DaaS)

- Amazon WorkSpaces
- Windows Virtual Desktop
- Citrix Workspace
- V2Cloud

Authenticator Apps:

- Authy
- Google Authenticator
- LastPass Authenticator
- Microsoft Authenticator

Business Anti-virus:

- McAfee Total Protection
- Malwarebytes
- Trend Micro
- ESET

Mobile Security:

- Scalefusion
- Lookout
- Jamf Pro
- KACE

Phishing Education

- knowbe4
- Phin Security
- Jigsaw | Google Phishing
- Phishingbox

CTSBDC@uconn.edu

www.ctsbdc.uconn.edu

(877) 723-2828