Cyber Hygiene, Tech Check Ups
The ASBDC North Star Cybersecurity Program will provide a baseline to promote cybersecurity awareness across ASBDC stakeholders, the national network and the SBDC client base. This baseline will allow flexibility within each of the 62 SBDC Networks while maintaining standards-based content, resources and programming to supplement current cybersecurity efforts.

**Deliverable:**

Business owners that are “cyber-aware,” practicing effective cyber/data hygiene and positioned to take continued steps toward self or third-party attestation, or formal certification.
The SBDC network, at its core, focuses on the tools and knowledge needed to grow and sustain a strong small business community across the U.S. and its territories. This is accomplished through one-on-one consultations, training and resource development focused on the primary functions of doing business like financial management, strategic planning, operational efficiencies, marketing and the application of technology. **Cybersecurity** services will build upon and strengthen these primary functions.
The North Star

- Utilizes the collection of existing frameworks and standards
- Core programming built from CMMC 2.0 and NIST while also mapping to other frameworks
- Consists of 6 domains
  - Access Control
  - ID & Authentication
  - Media Protection
  - Systems & Information Integrity
  - System & Communication
  - Physical Protection

CMMC

800-171

www.AmericasSBDC.org/Cybersecurity
The content contained within this presentation and any supporting documentation is meant for the purposes of learning basic cybersecurity awareness. It is not meant to provide or imply any form of certification within the CMMC, NIST or other regulatory model or framework. We hope you find this information useful in gaining a general understanding of basic cyber hygiene.

Should you require a more formal path to certification, the America’s SBDC Cybersecurity Task Force is able to provide several sources of professional training, consulting and assessment from within our group of sponsors and resource providers.
Welcome – Panelist Introductions

Jake Blacksten
Delaware SBDC
Digital Solutions Manager
Jacobb@udel.edu

Aikta Marcoulier
SBA
Region VIII Administrator
Aikta.Marcoulier@sba.gov

Dr. Shawn Murray
Chief Academic Officer
Murray Security Services
Add email
Agenda

1. What is Cyber Hygiene?
2. How do you conduct a cyber hygiene check up?
3. What are the steps of cyber hygiene?
4. Class Activity – hygiene tech check!
What is “Cybersecurity”?

Terminology
Cybersecurity is the new "sexy" term for information security.

Focus
While the focus appears to be primarily related to the IT systems, most IT security professionals agree that all aspects of Information Security are encompassed into this new discipline "brand".

Agreements
Includes contractual agreements for service providers of IT and cybersecurity.

• Many small businesses hire people or companies to provide these services which introduces risk.
• Who has access to your data and information?
• Do you have Non-disclosure Agreements (NDAs)?
Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.

Source: Digitalguardian.com
Cyber Hygiene – The Benefits

Having a routine cyber hygiene procedure in place for your computers and software is beneficial for two distinct reasons – maintenance and security.

Maintenance is necessary for computers and software to run at peak efficiency. Files become fragmented and programs become outdated, increasing the risk of vulnerabilities. Routines that include maintenance are likely to spot many of these issues early and prevent serious issues from occurring. A system that is well-maintained is less likely to be vulnerable to cybersecurity risks.

Security is perhaps the most important reason to incorporate a cyber hygiene routine. Hackers, identity thieves, advanced viruses, and intelligent malware are all part of the hostile threat landscape. While predicting threats can be challenging, preparing and preventing them becomes feasible with sound cyber hygiene practices.

Source: Digitalguardian.com
DON'T GET DUPED!

CYBERSECURITY HYGIENE CHECKLIST

DEPLOY MULTI-FACTOR AUTHENTICATION (MFA)

- Don't rely on just one layer of protection.
- Make sure your accounts have MFA enabled.
- Use a different device or method for each MFA type.

UPDATE YOUR SOFTWARE REGULARLY

- Keep your systems up to date with the latest patches.
- Regularly review and update your software.
- Stay informed about software vulnerabilities.

PASSWORDS—MAKE THEM STRONG

- Use a variety of characters and numbers.
- Avoid using the same password for multiple accounts.
- Change passwords regularly.

ENCRYPT AND BACKUP YOUR STUFF

- Protect your data with encryption.
- Keep backups of important files.
- Use cloud-based storage for added security.

DON'T CLICK ON THINGS YOU SHOULDN'T

- Be cautious of unsolicited emails.
- Avoid clicking on suspicious links.
- Double-check before entering sensitive information.

ADDITIONAL TIPS AND TRICKS TO CONSIDER

TIDY UP YOUR DEVICES AND REMOVE DIGITAL EXCESS

- Regularly clean out your computer and phone.
- Remove unnecessary files and apps.
- Keep your devices updated with the latest security patches.

REINFORCE YOUR SECURITY

- Use a strong password for each account.
- Enable two-factor authentication where available.
- Keep an eye out for new phishing and malware threats.

NOTES

www.AmericasSBDC.org/Cybersecurity
Deploy Multi-Factor Authentication (MFA)

MFA is an authentication process requiring two or more methods in order to get access.

MFA makes it harder for criminals to hack your passwords and accounts.
Update Your Software Regularly

Updates replace old versions of software with new versions that improve functionality and security.

Web browsers, MS Suite, Video Conferencing Apps, and others
Passwords – Make Them Strong

**DUPED**

**Complexity**
A minimum of 3 of the following 4:
- Upper-Case Letters
- Lower-Case Letters
- Numbers
- Symbols

**Lockout**
10-minute lockout after 8 unsuccessful login attempts (if possible to customize)

**Reuse**
No reuse of the last 6 passwords

**Change Frequency**
Passwords are changed every 90 days

**Length**
At least 12 characters

- Strong passwords stop criminals from hacking your accounts
- No Dictionary words
- No words turned into symbols
- Lie on Secret Questions
- Password Safe Programs
Encrypt and Backup Your Stuff

- Encryption securities a file or email by requiring a password to open it.
- Another layer of defense
- Only the right person can open up the file
- Encrypt data in the cloud
- Encrypt data at rest and in motion
- Website Encryption
Don’t Click on Things You Shouldn’t

DUPED

- Hackers will trick you with legitimate looking emails (spam, phishing)
- Identify suspicious emails and don’t click on links
What You Can Do At Your SBDC

- Host a cyber hygiene workshop
- Use the checklist in your consulting
- Join the cyber interest group
- Create a quick webinar
- Host a community cyber day
- Include cyber tips in all SBDC presentations
Sample Cyber Day

There's a hacker attack every 39 seconds! Don't be the victim! Bring your device (laptop, pad, tablet) for a free cyber hygiene check up by a cybersecurity expert. No sales, strictly an educational event for our community!

OCTOBER 19, 2021
9 AM - 3 PM

HTTPS://BIT.LY/CSCYBERDAY

www.AmericasSBDC.org/Cybersecurity
Class Exercise - Agenda

1. Software Update
2. Check Passwords
3. Are your emails encrypted?
4. Clean up browser settings
5. Check your social privacy settings
Software Update

- macOS Update
- Windows Update
- iOS Update
- Android Update
- Browser Update
Two Factor Apps & Password Managers
Thank You!