Get Going Guide

Keeping You and Your Business Safe Online

Four Simple Strategies to Increase Your Cybersecurity Readiness

Wyoming SBDC Network

Welcome!

The Wyoming SBDC received funds from the U.S. Small Business Administration to provide cybersecurity programs and resources to entrepreneurs across the state. Making your business cyber ready isn't just about using technology solutions; over 90% of cyber-attacks occur due to human behavior. Our approach to making you safer online focuses on adopting better habits, continuous training, and consistent communication. This program focuses on four core areas to make you and your business more cyber ready:

- Passwords
- Email/Phishing
- Software Updates
- USB Storage and Backups

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

Stephane Nappo, Global Head of Information Security for Societe Generale International Banking

"There are two types of companies: those who have been hacked and those who don't yet know they've been hacked."

Attributed to several individuals

"Companies waste millions of dollars on firewalls, encryption, and secure access devices; none of those measures address the weakest link in the security chain."

Kevin Mitnick, The World s Most Famous Hacker

> **"Cybersecurity grantees will help our small businesses avoid dangerous cyber-attacks that can create costly disruptions to their businesses and our nation's supply chains and digital infrastructure."**
>
> — *SBA Administrator Isabella Casillas Guzman*

Cybersecurity and Small Businesses by the Numbers

61% of small businesses were the target of an attack in 2021.

Small businesses receive the highest rate of targeted malicious emails (1 in 323).

87% of small businesses have customer data that could be compromised in an attack.

27% of small businesses with no cybersecurity protections at all collect customers' credit card information.

50% of small businesses said it took 24 hours or longer to recover from an attack.

Cybersecurity and You

How safe do you feel your business is online (website, customer data, email usage)?

○ Not safe at all

○ Somewhat unsafe

○ Not sure

○ Somewhat safe

○ Very safe

How comfortable are you implementing cybersecurity technology solutions on your own (password manager, firewall, antivirus software, etc.)?

○ Not at all comfortable

○ Somewhat comfortable

○ Very comfortable

○ Not sure

Have you or your business ever experienced a cyber-attack (phishing, virus, data breach, etc.)?

○ Yes

○ No

○ Not sure if I've been attacked

How would you describe how well your systems currently work (software, hardware, phone, etc.)?

○ Have moderate/serious issues

○ Have some issues but everything is functional

○ Confident that things are running well

Would you feel your business is safer online after some basic cyber readiness training?

○ Yes

○ No

○ Not sure but I'm interested in learning more

Quick Digital Assets Inventory

Internet enabled and connected hardware devices:

Internet Service Provider (ISP) and equipment (brands and models):

Have you ever changed your router's admin password?

○ Yes ○ No

○ Not sure

Who owns your website domain name?

○ Myself

If domain owned by someone else, enter name here

Cloud hosted services (e.g., banking, accounting, cloud backup):

Cybersecurity Vision and Goals

Company Mission Statement:

Cybersecurity Vision (to support mission statement):

3 5 Cybersecurity Goals (what you would like to accomplish as a result of this advising):

The Four Core Areas

Passwords

- Length
- Strength
- Management
- Security

Email/Phishing

- Know the danger signs
- Suspicious links
- Attachments
- Firewall advantage

Software Updates

- Automatic
- Up-to-date
- Hackers never quit
- Trusted providers

USB Storage/Backups

- Virus awareness
- Security/accessibility
- Backup frequency
- Disaster & recovery

Core Area 1: Passwords

A password is literally the key hackers use to get into your system. Following a few simple principles and habits will make your systems substantially more secure.

Why is better password management important? Verizon reports that in 2021 50% of all cyber-attacks were made with stolen login credentials.

Password Best Practices

- **Use long passwords** (15 characters). The shorter the password, the easier it is for hackers to break it.
- **Use a mixture of lowercase, uppercase, symbols, and numbers.**
- **Do not use self-identifying information in a password** (street name, pet's name, family member's name).
- **Do not use the same passwords across different accounts.** If a hacker finds a password on one site, they can get into all your others.

More Password Considerations

- **Consider passwords on all Internet-capable devices** (smart speakers, printers, robotic vacuums, appliances, etc.). Use the same best practices on all devices.
- **Use PINs and other available authentication methods on cell phones.**
- **Consider a password manager.** There are pros and cons but a good password manager can generate, store, and secure all passwords under one master access point. Do not use a web browser to generate and store passwords and payment information. Browser security is unpredictable.

Describe your organization's current password habits and guidelines.

What changes might you make to your organization's current password habits and guidelines?

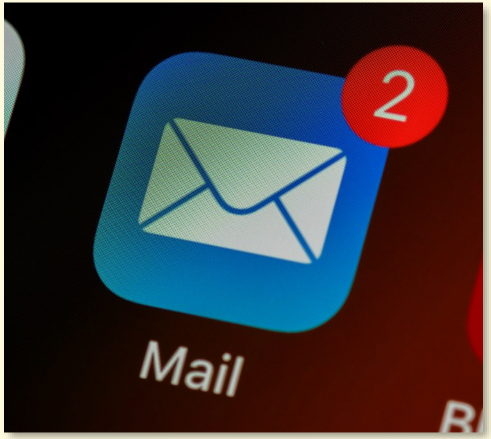
Core Area 2: Email/Phishing

Your email inbox is a front door for hackers and spammers. Email scams and phishing attacks only work if a person takes action on them. Behavior change and good habits are the best ways to combat those attacks.

Currently, 1.2% of all emails sent are malicious. That's 3.4 billion unsafe emails sent every day.

Email Best Practices

- **Enable email filters**. Many email scams are easily recognized as Spam by filters.
- **Consider the source.** Ignore, delete, and filter any email from an unknown source that contains a request.
- **Confirm the source.** Even if you know the name of the person sending an email with a request, call them to confirm before taking any action.
- **Activate your firewall.** A firewall won't block suspicious emails but it can prevent an attack on your computer if you happen to click a malicious link.



What are your organization's current guidelines for using email safely?

Let's Talk Phishing

- **The goal of a phishing email is to appear legitimate.** Carefully check the email address of the sender. The domain often resembles a real sender (goog1e.com, for example). If the address does not look legitimate, delete it and filter the sender.
- **Phishing emails are usually worded to reward or scare you.** A message may ask you to follow a link for a reward or warn you that your bank account has been compromised or something is wrong with your computer. Don't fall for it.
- **Senders are sloppy.** Although bad actors are getting better at their craft, a phishing attempt often contains odd formatting, misspelled words, or poor grammar.
- **I've been hacked. Now what?** Immediately report the incident to your IT professional. If you don't have IT support, follow these steps:
  1. Disconnect your computer from the Internet.
  2. Back up important data.
  3. Run an antivirus and malware scan.
  4. Depending on the severity of the attack, set up credit bureau fraud alerts and report the incident to the Federal Trade Commission.

Core Area 3: Software Updates

Software updates are usually inconvenient but always vital. A software update not only often contains feature upgrades, it usually fixes vulnerabilities that hackers might exploit. And hackers are always looking for new ways to get into your system. Accepting software updates helps keep your system secure.

According to the Cyber Readiness Institute, 37% of intrusions in 2021 began by hackers entering through a known weakness in program code.

Software Updates Best Practices

- **Accept update requests.** Programs always want to update when it's least convenient for you. Skipping updates puts your system at risk.
- **If you can't accept an update, schedule it.** Many updates allow you to schedule them for a downtime that is convenient for you.
- **Do not forget your phone and apps.** Keep your phone's OS updated and check often for app updates.

Software Tips and Tricks

- **Choose software from reputable vendors.** Ensure that the platform is regularly maintained and updated. Don't install freeware or software that looks sketchy.
- **Use a monitoring program to scan for available updates.** Such features are often included in antivirus suites.
- **If you no longer use a piece of software, delete it.** If you don't regularly use a program or app, you probably won't pay attention to updates. An unpatched piece of software is a welcome opening for a hacker to find.

What are the most important software platforms or apps to your business?

What measures do you take (or should you take) to ensure your most important programs are current with updates?

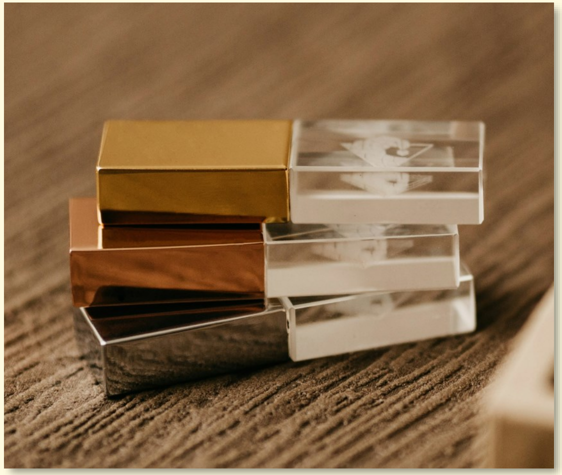
Core Area 4: USB Devices and Backups

USB storage devices are convenient, but they can easily carry viruses. USB drives are great trade show giveaways, but don’t trust that they are safe.

Data backups are often an afterthought, but they are your only option if your system is compromised. Once your data has been damaged or deleted, a backup is the only way to restore it.

USB Best Practices

- **Do not use USBs or removable media devices unless there is a business critical reason to do so.**
- **If you must use USBs or removable media devices take precautions.** Use antivirus software on your machine to scan external devices before use.
- **Never use “found” or “gifted” USB drives.** Hackers have been known to pre-load USBs with viruses and leave them around to be picked up and used by others.
- **If you are infected by a virus from a USB, remove your device from the Internet and scan it.**



What are your organization’s current guidelines for USB devices and backup systems?

Backup Basics

- **Use cloud storage for backups.** Choose a reputable cloud storage provider and schedule a regular backup routine.
- **Use auto encryption.** Most cloud storage providers allow you to automatically encrypt your backup data. In the event the provider is hacked, your data will be unusable by the attacker.
- **If you must back up on physical media, keep it protected and secured.** Some people will never trust the cloud for backups. If you need to use physical media, follow these steps:
  1. Create a regular backup schedule and stick to it.
  2. Disconnect your computer from the Internet during backups.
  3. Disconnect your media storage device when the backup is completed.
  4. Keep your physical backup in a locked, fireproof location.
  5. Consider keeping your backup at a secure facility other than your own location or make two backups: one to keep at your site and another to keep offsite.

Action Plan: Part 1

Based on what you've learned in this guide, what cybersecurity behaviors would you like to change in your business?

What solutions can you put in place?

Action Plan: Part 2

List tasks to be performed, in priority order (most important first) and who will be responsible for each:

Create a timeline for when tasks will be completed (e.g., Tasks 1 3 to be completed by May 15):

Credits and Notes

Photo credits:

Cover photo: Linked in Sales Solutions, Unsplash.com

Page 2:	Blake Wisz, Unsplash.com
Page 8:	Kenny Eliason, Unsplash.com
Page 9:	Brett Jordan, Unsplash.com
Page 10:	Austin Distel, Unsplash.com
Page 11:	Jonathan Borba, Unsplash.com

Content credits:

Much of the information in this guide is based on the Cyber Readiness Institute's "Cyber Readiness Program." Two levels of self-paced cybersecurity training can be accessed for no cost at cyberreadinessinstitute.org

Phishing attack recovery steps on page 9 are based on those found at this url: https://www.eloan.com/blog/personal-finance/7-steps-to-take-now-if-youre-a-victim-of-a-phishing-attack

The guide was developed by the Wyoming SBDC Network and is intended for use by its clients. Development of this guide was funded through a Cybersecurity for Small Business Pilot Program grant from the U.S. Small Business Administration.