SECURE OUR WORLD

ACTSMART I.T.
Helping You Benefit From Today's Technologies

Four Easy Ways to Protect Your Business

2023 CHAMPION
CYBERSECURITY AWARENESS MONTH

You Can Protect Your Business from Online Threats

Your business is digitally connected—to employees, vendors and customers. Your systems store sensitive information. Sensitive business information and customers' and employees' personal data could be at risk from online threats. No business is too small to be a target for online crime—the fact is, small businesses are much more likely to be targeted by cybercriminals than larger companies.

Did you know that a majority of small and medium-sized businesses who suffer a cyberattack often close as a result? It's hard to recover financially from a cyber-attack. This doesn't have to happen to you!

CISA.gov (Cybersecurity and Infrastructure Security Agency) recommends four simple steps you can take to make your business MUCH SAFER from online dangers.
Secure your business...Secure Our World.

Even just practicing the basics can make a huge difference.

#1 RECOGNIZE and AVOID PHISHING

Harmful links or attachments could provide unauthorized access to information or infect your network with malicious code. This can result in data being held for ransom.

Most successful online attacks begin when someone clicks and downloads a malicious attachment from an email, direct message or social media post. These phishing attempts can result in stolen passwords that criminals can use to log in to sensitive accounts to steal data or money. Phishing can also result in the user unwittingly downloading malware that damages systems or installing ransomware that holds systems captive.

#2 USE STRONG PASSWORDS AND A PASSWORD MANAGER

Passwords are the keys to your digital castle. Just like your housekeys, you want to do everything you can to keep your passwords safe.

PASSWORDS - LONG, UNIQUE, COMPLEX

No matter what accounts they protect, all passwords should be created with these three guiding principles in mind:

- Long – Your passwords should be at least 12 characters long.
- Unique – Each account needs to be protected with its own unique password. Never reuse passwords. This way, if one of your accounts is compromised, your other accounts remain secure. We're talking really unique, not just changing one character or adding a "2" at the end – to really trick up hackers, none of your passwords should look alike.
- Complex – Each unique password should combine upper case letters, lower case letters, numbers, and special characters (like >,!?). Again, remember that each password should be at least 12 characters long.

As our online lives expand, we've gone from having just a few passwords to today, where we might manage upwards of 100. That's 100 unique passwords to remember if you use strong passwords. Password managers can save users many headaches and make accounts safer by recommending strong passwords.

#3 ENABLE MULTI-FACTOR AUTHENTICATION

What is multi-factor authentication?

Multi-factor authentication is sometimes called two-factor authentication or two-step verification, and it is often abbreviated to MFA. No matter what you call it, multi-factor authentication is a cybersecurity measure for an account that requires anyone logging in to prove their identity multiple ways. Typically, you will enter your username, and password, then verify your identity some other way, like with a fingerprint or by responding to a text message.

It might seem like a lot of work, but once you set up multi-factor authentication, proving your identity usually adds just a second or two to the login process. And the peace of mind that multi-factor authentication provides is well worth it.

We recommend implementing multi-factor authentication for any account that permits it, especially any account associated with work, school, email, banking, and social media.

#4 UPDATE YOUR SOFTWARE

Flaws give criminals an opening. Programmers publish patches, but you must install them to get their protection. Smaller businesses are often running outdated software because they don't have full-time IT staff keeping up.

This Cybersecurity Awareness Month, we're telling everyone to step away from the "remind me later" button to stay one step ahead of cybercriminals.

Recently, the Cybersecurity and Infrastructure Security Agency (CISA) launched a new nationwide, year-round cybersecurity program to educate all Americans on how to stay secure online. ACTSmart IT is proud to be a part of that program!

For FREE Weekly Security Tips Emailed to You and Your Team, go to:
https://actsmartit.com/tips/