SMALL BUSINESS BIG THREAT

Small Business, Big Threat

Online Security Best Practices

Background & Introduction

The following document is intended to assist your business in taking the necessary steps needed to utilize the best security practices for your employee's devices and to help them in protecting business information and their own personal information while browsing the internet.

The document discusses the most basic security practices that **ALL** businesses should be following as a baseline. If you feel you fall into a more complex category it is highly recommended that you contact your IT service provider for further guidance and assistance.

This is not a comprehensive list of all possible security procedures, as many advanced IT security needs depend on the nature of your business and whether or not your business has industry compliance requirements

Passwords

- Enable Passwords/PINs/Lock-out settings on your computer, phone, and tablets. If you don't have them, anyone who takes your device now has access to all your data & accounts. Remember to lock your devices if you leave them.
- Passwords should include a max of upper & lowercase letters, numbers, and special characters.
- Password length is better than password complexity, and is your only defense against hacker "brute=force" attacks (guess your password by systematically trying every possible combination).
- To easily make your password twice as long, very complicated, but still easy to remember & type, consider entering every single character of your password twice. For instance: cat = ccaatt
- Passwords should be unique; you should NEVER use the same password for multiple sites/services. Otherwise, if a low-security site gets hacked, the hacker now has access to all your other sites/services.

Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

Small Business, Big Threat

- If passwords must be written down, they should be stored in a locked and physically secure location (not hidden near the computer desk). If passwords must be saved on your computer, they should not be stored in a document/spreadsheet on your computer, but should instead be stored in a "password manager" tool, so all your passwords are encrypted with a master password.
- "2 Factor Authentication" is better than only a password protecting your account. Example: Factor 1 is something you know (your password); Factor 2 is something you have (such as a text message sent to your phone). If you have "2 Factor Authentication" enabled, a hacker with your password is powerless without the special message to your cell phone.

Data Backups

- If the data only exists in one sport, it is not a proper "backup". Computers fail. External drivers also fail or get stolen.
- Test and verify your backups by restoring a test file at least once a year, preferably once a quarter.
- Regular backups are necessary; malware exists that will encrypt all data it can find on a computer with an unknown password and hold it for ransom until you pay.
- Cloud backups are a good salutation, but first read the cloud services details if data confidentially is needed, since not all cloud backup services encrypt the data.

AMERICA'S SBDC MICHIGAN
MEDC MICHIGAN ECONOMIC DEVELOPMENT CORPORATION
PURE MICHIGAN Michigan Economic Development Corporation
U.S. Small Business Administration SBA Your Small Business Resource
Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

Credit Cards

- If your Credit Card ever gets stolen: 1) immediately contact your credit card company and report it stolen, 2) have them reissue a new Credit Card number, and 3) monitor your monthly statements for false charges. Act immediately to report it and the Credit Card company should be able to reverse any fraudulent charges.
- If your company accepts Credit Card payments, establish Workplace Policies to train employees on proper Credit Card handling.
- If you must write down Credit Card numbers, it should be written on a specific color of paper, the paper should be stored in a locked and secured location, and all paper must be destroyed & shredded before being discarded.
- Credit Card numbers should NEVER be stored in plain-text on a computer or server that is not encrypted and protected by a complex password.
- Credit card numbers should never be sent by e-mail, as normal e-mails are not encrypted.

Small Business, Big Threat

Wireless Internet

- Be very careful when connecting to unknown open wireless networks. If you must use one, make sure it is a legit wireless network (and not fake WiFi by a hacker), confirm your internet traffic is encrypted by examining the security certificate of all websites in order to make sure your traffic has not been manipulated with.
- When configuring your own Wireless Network, change the network name (SSID) to something unique (that does not give any personal identifying information), enable Wireless (WPA2) encryption, and use a long, complex, and unique wireless password (be sure to follow the Password Best-Practices listed above).
- When configuring your own Wireless Network equipment, change all equipment login passwords (be sure to follow the Password Best-Practices listed above).
- When configuring your own Wireless Network equipment, check with the device manufacturer regularly for updates, since network equipment often also has flaws (similar to computers).

AMERICA'S SBDC MICHIGAN
MEDC MICHIGAN ECONOMIC DEVELOPMENT CORPORATION
PURE MICHIGAN Michigan Economic Development Corporation
U.S. Small Business Administration SBA Your Small Business Resource
Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

General Device Maintenance & Security

- Every computer, smartphone and tablet vendor has software flaws and requires regular updates.
- Do not delay application and operating system updates; this often causes problems or is what allows a system to become compromised.
- Restart most devices weekly to apply updates, refresh your application, and check for new updates.
- Run only approved security software; research all security software before installing; hackers have released fake security software in the past.
- Your security software should include (at a minimum) malware/virus detection and website content filtering.
- Website content filtering is important since many viruses today are spread by tricking you into visiting a compromised website that exploits a flaw in your browser in order to load malicious software on your device. Be careful which website links you click on!
- Running security software does not mean you are protected from new viruses; anti-virus software only helps detect "known" viruses. There are too many unknown viruses being created to catch them all. Be careful what files run and what apps you install!

Small Business, Big Threat

- Research all smartphone/tablet Apps before installing; hackers have been known to release fake look-alike Apps in order to compromise devices.

Security Awareness

- Hackers are known to call people and pretend to be "Tech Support: in order to trick you into giving them access to your device, open a strange email attachment, have you go to their compromised website, or into gibing out your password. A healthy suspicion of this type of behavior may help you identify malicious attempts.
- If you receive an unsolicited phone call, ask them for their name, their organization, and a number to call them back after you research them. If they do not give you this information be very suspicious. Research the company to make sure the number they gave you is legitimate. Be careful about the information you give them without confirming their identity.

AMERICA'S SBDC MICHIGAN
MEDC MICHIGAN ECONOMIC DEVELOPMENT CORPORATION
PURE MICHIGAN Michigan Economic Development Corporation
U.S. Small Business Administration SBA Your Small Business Resource
Developed by Michigan SBDC with support from the U.S. Small Business Administration and the Michigan Economic Development Corporation

- Be careful about what data you place on your website and social media; an attacker may use this information to compromise your network or trick your employees.
- Security is a “process”; not a “product”. There is no single piece of software or single piece of hardware that can make you “secure”.
- Even if you do not consider your data sensitive or confidential, your device and personal information can be used by a hacker to launch attacks or commit fraud.
- Technology “security” can be achieved by having awareness of the risks, following best-practices as suggested by security experts, and by making good technology decisions.

Advanced Business Security

- If you have Servers on-site at your company, the Servers should be configured on a dedicated network segment, protected by an internal firewall device, since client devices surfing the Internet are often the first devices to get compromised and can more easily compromise your Servers if able to access them directly.
- If client devices are travelling with sensitive data, the entire device storage should be fully encrypted and protected with a long & complex password.
- Physical security of your equipment is critical. If an attacker can get physical access to your computer or server, they will be able to compromise it (eventually.)