https://BrianAlawayConsulting.com

5 Cybersecurity Tips for Small Business

Cybersecurity tips to protect your small business in the digital economy.

Here are **5 Cybersecurity tips** to protect your business from online disaster. Whether intentional or accidental, follow these basic tips and you'll be light years ahead of most small businesses in terms of cybersecurity and protecting your business.

1. **Record critical user names and passwords**. Create a spreadsheet containing the following information and store a digital copy it in a safe location (encrypted on disk) and a paper copy (safe or bank box). You MUST have control of all of the above. Do NOT trust your web guy/gal/designer etc. to own this. If you part ways you will need to have this information and the ability to change or update as required. NO EXCEPTIONS.

Domain name registrar ______________________________

- web address url ______________________________
- Login **username** ________ and **password** ______________________

DNS management provider ______________________________

- web address url ______________________________
- Login **username** ________ and **password** ______________________

Server management ______________________________

- web address url ______________________________
- Login **username** ________ and **password** ______________________

W**ebsite host** ______________________________

- web address url ______________________________
- Login **username** ________ and **password** ______________________

Website login ______________________________

- web address url ______________________________
- Login **username** ________ and **password** ______________________

Email admin ______________________________

- web address url ______________________________
- Login **username** ________ and **password** ______________________

Note: **Domain name registrar** and **DNS management provider** may be the same but often are not. Example: Domain name registrar name (e.g. godaddy.com, siteground, com, etc.) but DNS management is provided by your Website host or a third party proxy service like Cloundflare.com. Also, some Domain Name registrars may also be your **Website host** (e.g. Namecheap.com). If you use a content management system like WordPress, your **Website login** will be to your admin dashboard, typically https://<yourdomain>.com/wp-admin. Your **Email login** could be via your **Server management** (e.g. cPanel and/or WHM) or a third party such as gmail.com or yahoo.com. This is why you must discover answers to the above and record them.

2. Use a **unique and difficult to hack password for each** of the above. *NEVER* use the same password to access multiple different logins. This will limit the damage possible should your password for any one login become compromised (hacked). When creating your passwords keep these points in mind:
    - Longer is better. The longer the password, the longer it will take for a brute force password attack to be successful. Here's a graphic to better understand how length matters and is more important than complexity: https://xkcd.com/936/
    - Rather than trying to remember a long combination of random characters, numbers and symbols, think in phrases. A phrase is much more memorable. Here's an example: a horse of a different color. Easy to remember the phrase but now just switch it up to create this password phrase: a different colored horse.
    - But what if you have dozens of passwords for different things? Time for a password manager. A password manager will create and store multiple passwords, auto-fill logins and forms and automatically create not only very long passwords but also very complex passwords. You will only need one Master Password to access all your stored passwords. Use the phrase method to create your master password. Make sure the phrase is at least 12 characters long, preferably longer. Here's an example: the cow jumped over the moon the dish ran away with the spoon. Switch it up to create this password phrase: spoon away the dish moon the cow
    - Again NEVER use the same password for more than one email, one website, one anything.
3. **Enable two-factor authentication** for all of the above if possible. Two-factor authentication is an extra layer of security used to verify the identity of anyone attempting to gain access to any of the above. This ensures that should your username and password become compromised, the intruder will still have to verify the second security layer in order to gain access. Check with your service provider to see if and what types of two-factor authentication is available. There a several types of two-factor authentication but the two most common are

   - a time-limited code is sent via phone or SMS text message. You enter the code given to verify your identity and gain access. Since this code must be transmitted over the third party network, it's considered less secure than the next method.
   - a push notification is sent to an app on your web connected device. You then approve or deny with a single touch. Since this requires that your device be connected to the web, it's best to have phone or SMS verification as a fall back.

4. Determine what data is critical to your business operation and protect it by:
   - Limiting access to this data. Don't give access to critical data unless that person cannot perform their job function without access. Instruct all your employees to not click on links in emails or download attachments from email or websites unless they are expecting the attachment and trust the sender. They can always contact the sender FIRST to verify if in fact they sent the message/link/attachment.
   - Requiring all company devices used to connect to the internet MUST have UP TO DATE anti-virus and/or malware protection. Schedule a weekly or monthly group timeout to make sure all security software is active and up to date. This includes all mobile devices as well as computers. If you allow employees to use their personal devices for company access, make sure these are also protected.
5. **BACKUP**, BACKUP, BACKUP! Make sure that any critical information, whether it's stored locally or online, is backed up on a consistent schedule. The most secure backup policies store backups both locally and online. If your business employs an onsite server, critical information should be stored on the server NOT individual devices. The most critical data can then be copied to an attached storage device and stored in a DIFFERENT secure location, Ideally, this should be in addition to any online backup storage. Remember, if physical disaster (think fire, flood, hurricane, tornado, etc.) strikes your facility or area you may lose your onsite server and you may or may not have online access to download your backups. Even with online access, large data backups could take hours, days or even longer to access. **Think redundancy**.

BONUS TIP: Include the cybersecurity tips above as part of a complete disaster recovery plan.

BONUS Resources:
Disaster Preparedness and Recovery Plan from **SBA**
https://www.sba.gov/document/support--disaster-preparedness-recovery-plan

The Best Free Antivirus Protection of 2018
https://www.pcmag.com/article2/0,2817,2388652,00.asp

Free Online Storage
https://www.moneysavingexpert.com/shopping/free-online-storage/

The best Windows backup software
https://www.pcworld.com/article/3201971/software/best-windows-backup-software.html