Cybersecurity basics you shouldn’t ignore.

7 Cybersecurity basics to never forget

No matter how much people hear “data safety,” they still can get sloppy about their cybersecurity. One of the reasons is that there are so many constant reminders that the warnings just become that much more background noise. Also, when it comes to smaller and medium sized businesses, anything that distracts from the day to day concerns about bringing in revenue tends to fall by the wayside. With that in mind, we have put together a list of seven things that a small business needs to prioritize if you want to keep your business up and running. Remember, a cyber attack on your data security could be the biggest threat to your revenues that you face, even more serious than a recession or a pandemic.

Passwords

As annoying as they are (and who doesn't doest curse them sometimes) passwords are a basic and necessary evil to protect access to your data. One of the root innovations that helps sidestep the tedium of entering (and remembering) passwords are facial recognition and fingerprint security measures. These can be a real timesaver, but they aren't readily available across every site and device. So that leaves us with the question, what are the best practices for maintaining strong passwords and defending multiple sites, programs or devices (also known as “ good password hygiene’’)?

Maintaining password best practices

Simple passwords, with nothing but regular vocabulary words (even in other languages) are easily cracked. Most sites generally require mixed case, alphanumeric and a symbol or two for it to be an approved password. Here are a few things to remember.

- Avoid using the same password across multiple sites or devices.
- Don’t share your passwords with co-workers, no matter how convenient or timesaving it may be
- Don’t send passwords (or any critical personal data, for that matter) via text or email.
- Don’t save them on a device in an unencrypted file
- Remember to change them periodically
- Be sure that access to files is removed immediately when an employee leaves an organization or no longer has need to access particular programs, data or machines

Multi-factor authentication

Related to the password method of maintaining data security, multi-factor authentication is becoming increasingly popular and is often required by some organizations. Basically, this takes the password idea and adds another layer to ensure that the correct user is entering the password. Your ATM is an example of MFA. Just a password isn't enough at the ATM--you have to have your ATM card also. Most of us know MFA through the request to enter a one time code that is sent to us, on a different platform, after we enter our usual password. Again the idea here is that even if a password is stolen, a second form of identification is required to ensure the correct person is gaining access. NOTE: A common form of MFA is to send a text message to your phone. Be aware that if you leave the country and don't buy a text package for your phone, you may not be able to access some sites that use this form of MFA.

Data encryption

This takes standard readable text (i.e. stuff that you and I can read, for example) and encrypts it so that it is unreadable. The recipient of the data needs a key to encrypt the data. For example, encrypted email means that when you send an email, it is automatically encrypted - unreadable to anyone who intercepts it - and it is not “decoded” until it hits the mailbox of the intended recipient. All business data should be encrypted no matter where it resides-smartphone, external drive servers, and routers.

Software

Everything you have uses software programs, all of which can be vulnerable to hacking.   Make sure all of your software programs are up-to-date. Software companies release program updates, security patches and critical updates for their applications. In addition to providing new features or fixing bugs in the program, these updates and patches prevent cybercriminals from exploiting the vulnerabilities that exist in the program to gain access to your network and data. So, you need to take the time to make sure that all of your software applications, including operating systems, and browsers are up-to-date. And do not forget your smartphone. It is important not to leave out your smartphone applications and mobile devices as well, because cybercriminals can find a way to invade your network and data from your smartphone For example, you have your work email configured on your phone. Hacking into your phone can give them access to your work email and consequently to work data.

Backups

There are things we all know we should do that are good for us, but that doesn't mean we do them. Eat your vegetables, exercise every day... and back up your data. So here is a reminder of what you should do. Make sure you have clean and up-to-date backups. Backups come in extremely handy, especially in the case of ransomware attacks. Ransomware attacks are where cybercriminals gain control of your network or data and lock you out of your own system preventing you from accessing crucial business data. Sometimes your data is encrypted, which means it won't be "legible." They then demand a ransom to unlock or decrypt your data. Unless you pay up, you won't have access to your data or your data won't make any sense to you as it is encrypted. Having up-to-date, quality backups ensures you don't have to worry about losing access to your data or paying the ransom, as you would have a most recent copy of your business data readily accessible. You can make backups on external hard disks, servers located at a place different from your place of business or even on the cloud (think Google Drive or One Drive or cloud servers). That said, contact an MSP to design workable backup procedures that don't include copies of the ransomware. Just routine backups may not be enough to protect you.

Train everyone in your organization

Never forget the human factor in how cybercriminals get through your defenses. Training your employees to identify and respond correctly to cyberthreats plays a big role in any organization's cybersecurity initiative. Regular cybersecurity training sessions along with mandated assessments should be conducted for all employees. Based on the assessment results, you may conduct follow-up training or refresher sessions for those who need it. You should also create an IT security policy document or handbook and share it with everyone in your company. This handbook or policy document must be updated on a routine basis to keep up with the latest in cybersecurity protocols.

Cybersecurity might seem like a lot of work, especially when you have a business to run and clients to focus on. However, it is certainly not an element that you can afford to ignore. The price you may have to pay if your business becomes a target of a cybercriminal is too high to take cybersecurity lightly. Consider bringing an experienced Managed Services Provider (MSP) on board to help manage the cybersecurity aspect of your business, while you can focus on your clients.

ALTERNIS® IT
DEVELOP. DELIVER. DEFEND.

For more information please contact,
Art Katch | Founder
Alternis IT
Phone: 408-987-8000
Email: art@alternisit.com
655 Montgomery St, STE 490 Dpt 17037, San Francisco, CA, 94111
https://www.alternisit.com