COLEMAN TECHNOLOGIES

The 5 Biggest Cybersecurity Risk & How to Protect Your Business From Them

At nearly $1 Trillion in earnings a year, the cybercrime business is now at record proportions. Hackers make big money from stolen data.

www.colemantechnologies.com

The following are the 5 biggest cybersecurity risks you must be aware of today:

1. Ransomware. There's been a huge increase in these attacks within the last year. CryptoLocker encrypts all of your data to prevent your access to it. Locker Ransomware locks your computer so you can't login. Even if you pay the ransom to get access (which you shouldn't), people are still being locked out.

2. Phishing is a targeted email attack. Favorite targets are financial corporations. The odds are good that phishing works – a campaign of 10 targeted messages has a better than:

- 90% chance of getting a click.
- 8% chance of users clicking on an attachment.
- 8% chance users will fill out a web form.
- 18% chance that users will click a malicious link in an email.

3. Social Engineering. This is where you get fooled into sharing passwords, bank information, and computer access codes. Believe it or not, this happens all the time; and when it does the cybercriminals can also copy your email list and send out a message in your name that has malware attached—So, your contacts' computers will also be infected.

4. Social Media Sites. Did you know that hackers insert malicious code into ads on Facebook, Twitter and other sites? For example, over 100 million Facebook users had their private information shared illegally when they clicked on a malicious pop-up ad.

5. Public Wi-Fi Hackers now emulate free open Wi-Fi to steal your IDs and passwords. You can be fooled when you try to login to free Wi-Fi in airports, restaurants and other public areas. When this happens, everything that you type can be copied and archived by these criminals, and used against you.

5 Steps You Should Take to Protect Yourself

Step 1: Ignore Ransomware-Threat Popups and Don't Fall for Phishing Attacks.

These threats look like they're from an official entity like the IRS or FBI. If a screen pops up that says you'll be fined if you don't follow their instructions, don't! If you do, the criminal will encrypt all your data and prevent you and your employees from accessing it.

Beware of messages that:

- Try to solicit your curiosity or trust.
- Contain a link that you must "check out now."
- Contain a downloadable file like a photo, music, document or pdf file.

Don't believe messages that contain an urgent call to action:

- With an immediate need to address a problem that requires you to verify information.
- Urgently asks for your help.
- Asks you to donate to a charitable cause.
- Indicates you are a "Winner" in a lottery or other contest, or that you've inherited money from a deceased relative.

Be on the lookout for messages that:

- Respond to a question you never asked.
- Create distrust.
- Try to start a conflict.

Watch for flags like:

- Misspellings
- Typos

Step 2: Always Use Secure Passwords.

- Never use words found in the dictionary or your family names.
- Never reuse passwords across your various accounts.
- Never write down your passwords.
- Consider using a Password Manager (e.g., LastPass or 1Password)
- Use password complexity (e.g., P@ssword1).
- Create a unique password for work.
- Change passwords at least quarterly.
- Use passwords with 9+ characters.
  - > A criminal can crack a 5-character password in 16 minutes.
  - > It takes 5 hours to crack a 6-character password.
  - > 3 days for a 7-character one
  - > 4 months for 8 characters
  - > 26 years for 9 characters
  - > Centuries for 10+ characters
- Turn on Two-Factor Authentication if it's available.

Step 3: Keep Your Passwords Secure

- Don't write down passwords.
- Don't Email them.
- Don't include a password in a non-encrypted stored document.
- Don't tell anyone your password.
- Don't speak your password over the phone.
- Don't hint at the format of your password.
- Don't use "Remember Password" feature of application programs such as Internet Explorer, Portfolio Center or others.
- Don't use your corporate or network password on an account over the Internet that doesn't have a secure login where the web browser address starts with **http://** instead of **https://** If the web address begins with **https://** your computer is talking to the website in a secure code that no one can eavesdrop on. There should be a small lock next to the address. If not, don't type in your password.

If you believe your password may have been breached, you can always change it.

Step 4: Backup Your Data Onsite/Remotely and Securely

- Maintain at least 3 copies of everything.
- Store all data on at least two types of media.
- Keep a copy of your data in an alternate location.

If you haven't backed up your data, and you're attacked, it's gone forever.

Step 5: Secure Open Wi-Fi with a VPN

- Don't go to sites that require your personal information like your user name or password.
- Use VPN whenever possible (You can purchase this device at: IPvanish.com).
- Limit your access to using sites with: https://
- Don't connect if all the Wi-Fi networks you have ever accessed appear as "Available."

Step 6: Hire a Reputable IT Company to Conduct Testing and Training

- Conduct a Social Engineering Test
- Share the Results with Your Staff
- Debrief and Train Your Users
- Test Again each Year!

Don't risk your data to cybercrime. Coleman Technologies will help you keep your data secure.

Our Cybersecurity Experts are always here to help. Contact us with any questions you have at info@coleman.biz or (604) 513-9428.