Don’t Fall Victim to a Cybercrime

Arm Your Firm With a Cybersecurity Protocol

1 Have the same data backup plan for all your firm's staff

Are you backing up sensitive information through a portal device or cloud-based storage? Ensure your backup operation is the same for everyone.

Also, make sure there’s a backup protocol in place: do you want to backup all your data weekly? Bi-weekly? Monthly? All the staff should be on the same page here.

2 Use multi-factor authentication (especially on Socials!)

Are you working with socials? Add a two-step verification. Google has an **authenticator app** for this.

3 Replace passwords with passphrases

Got any accounts with sensitive and confidential information? Use a passphrase! Make it at least 14 characters long and include a combinator of lower and upper case letters, numbers, and characters.

4 Did an employee leave or switch devices? Empty all old devices

Don't leave the backdoor open to hackers. Turn off the WiFi and Bluetooth on all old devices that aren't being used.

Don’t Fall Victim to a Cybercrime

Arm Your Firm With a Cybersecurity Protocol

5 Add security policies and educate your staff!

Your staff may be the first and last line of defense if a cyber threat happens, so make sure you have a protocol with the do's and don'ts when emailing, calling, acquiring a client’s banking details, social security numbers, etc.

6 Worst case scenario? Know who to call when and if a cybercrime happens

In the USA, you can (and should) report cybercrimes using the following 3 tools:

- CISA's (Cybersecurity & Infrastructure Security Agency) reporting tool
- FBI (Federal Bureau of Investigation) Internet Crime Complaint Center
- U.S. Secret Service Local Contact

At Consultwebs, we're not leaving any backdoors open for cybercrimes. Whether you're looking for a reliable agency, want to ask more questions, or secure all your marketing channels...

...we’re here to help out