cowbell®

Cybersecurity Recommendations for Businesses

Recommendations to Keep Your Business Safe in Cyberspace

In light of the increasing rates of cyberattacks, including cyber crime, ransomware, phishing, and other types of cyber incidents, it is imperative for your business to have a secure cyber perimeter and to practice basic cyber hygiene in order to be protected from cyber criminals.

Some examples of how you can implement good cyber hygiene practices include:

- Making sure that employees are using a VPN and MFA to log in to the company's systems and networks.
- Investing in cybersecurity tools to ensure that your and your clients' data is secure.

Hackers are expanding their activities online and are targeting small to medium-sized business in hopes of obtaining valuable financial and digital assets from companies.

Did you know? According to Verizon's 2023 data report,...

- Business Email Compromise (BEC) attacks have **almost doubled in the last year**
- **74% of breaches** involved the human element
- The three primary ways in which attackers access an organization are **stolen credentials, phishing and exploitation of vulnerabilities**.

Resources for Staying Safe Online

Here are some recommendations from the Cowbell team that can help your business stay safe online:

1 Multi-factor authentication (MFA):

Enable MFA on all services supporting it: payroll application, CRM system, online banking, email services, and more. Many software companies allow administrators to make MFA mandatory for all employees.

2 Patching:

Keep devices, applications, and website tools up-to-date and patched to the most recent versions of software.

3 Avoid using public WIfi:

Never use public Wifi to access sensitive data without a secure and private VPN. It is easy for bad actors to infiltrate systems when you are using the same Wifi connection.

4 Only visit secure websites:

A secure website will have an address that starts with https, not http. Most browsers will raise an alert on suspicious sites granted that you're running the latest browser version.

5 Revisit your loss mitigation strategy:

Review what your cyber insurance coverage includes or not, what type of event might be excluded. Check whether the limit, sublimits and deductibles you signed on for cyber still reflect the state of your business and your use of technology today.

6 Apply basic password hygiene:

Do not share passwords, do not reuse passwords, especially between personal and professional services. Do not write them on sticker notes. Create passwords that are as long as possible.

7 Cybersecurity awareness training:

A knowledgeable employee can mean the difference between a successful and an unsuccessful cyber attack. Developing a cybersecurity awareness training program for all employees is essential.

8 Don't hesitate to ask questions:

If you need clarification on Business Interruption / Business Income coverage, what is covered or not, feel free to contact us.

US0019 0224