FULLYMANAGED

TOP 4 CYBERSECURITY TIPS TO PROTECT YOUR BUSINESS.

Experts predict that over 50% of businesses will be the victim of a cyberattack in 2018.

While data breaches of enterprise organizations will continue to make the news, it's the small and medium-sized businesses that will really suffer. Without deep pockets to mitigate losses incurred from comprised data, a single attack could be enough to force you to close up shop.

What sort of losses could you face? Cyberattacks have led to everything from legal expenses, ransomware payouts, literal theft from company accounts, and more. This is the reason that 60% of hacked SMBs go out of business after six months of the attack.

While the threat is real, so are the solutions. Hiring a cybersecurity firm to manage your data is one, but there are also some do-it-yourself tips and tricks that you can apply to company protocol that will help keep you safe from cybercrime. The team at Fully Managed has compiled our 4 top tips to keep your business safe from cyberattacks in 2018.

1 Switch to a Secure Messaging App for Important Internal Communications

Make a pledge to stop confidential file sharing over email in 2018. By nature, email is insecure because it is sent over the internet. Even a low-level hacker with a packet analyzer (a program that intercepts and logs traffic that passes over a digital network) can grab your corporate email communications.

Your business may have switched to secure email, but even that is problematic. So-called 'secure email' takes the sender's clear text and encrypts the communication, then decrypts it from the inbox directly on the recipient's local computer. What secure email does not address is the fact that many copies of the communication are stored across the internet as backups. A single communication is generally available in your sent folder, in the recipient's inbox, and if they reply, it is also copied to their sent file, and so forth. The issue is compounded when email is connected to numerous devices that staff use on a day-to-day basis, storing communications on the computers, laptops, and smartphones of both the senders and recipients.

This redundancy of data communication puts it at great risk.

To hedge this risk, send sensitive communications over an encrypted messaging app. Unlike email, server-side applications such as secure messaging store the data centrally and in one secure location. You can't send a communication from one messaging app to another. Need an example? Try messaging someone from Signal to WhatsApp. It's not possible, even though they both share the same encryption protocol.

Encrypted messaging apps still perform backups, but because the data remains under the control of the vendor, it is not roaming haphazardly all over the internet.

We're not suggesting that you abandon secure email altogether, as you most certainly need it to communicate with current and prospective customers, but when it comes to sending sensitive information to staff and stakeholders, stick to a secure messaging app that offers end-to-end encryption.

2 Institute an Immediate Update Protocol for Systems and Software

Your business depends on computer systems and open source software for content, data, and customer relationship management, all of which are susceptible to hackers. Because of this, the open source community and software providers update programs to plug new holes in cybersecurity while vendors and manufacturers deliver firmware updates if an exploit is found.

However, far too often businesses neglect to perform the required updates. The reasons for not doing so are often ironic. The very updates that intend to protect businesses from cybercrime are not performed because the users are fearful that the notification request for an update is a scam that may open them up to an attack. If this is your concern, simply verify and get the update from your vendor's own website. If you're holding off on an update because you fear that it will result in a systems error, make an effort to get on the phone (or chat) with someone from vendor support.

Moving forward, pay close attention to all update alerts, verify their legitimacy with the provider, and promptly perform the update.

3 Freeze Hackers Out of Your WiFi HotSpot

If a hacker can access your WiFi there's potential for them to wreak havoc on your network.

Your business WiFi network should be kept secured and hidden from public view. In addition, make sure that your firmware is updated, and that staff WiFi passwords for password policy best practices and are changed quarterly. In addition, set up MAC authentication, a protocol which admits or denies wireless association based on the connecting device's MAC address (a computer's unique hardware number). MAC authentication will help keep the ill-intentioned from hopping onto your network, even if they happen to have access to the network name and password.

If you're a brick-and-mortar business that provides free WiFi for customers be sure to use a separate network for your own business operations (i.e. processing payments, etc.) which can be accomplished via network segmentation.

4 Enforce Best Practices Regarding Password Policies

When it comes to cybersecurity, the most obvious protective measure is the most effective. The annual Verizon Data Breach Investigations Report (DBIR) for 2017 states that 81 percent of hacking-related breaches succeeded through stolen or weak passwords. Even more concerning, is that the figure shows an 18 percent increase from last year's report, indicating that even with all of the focus on passwords, password security is actually getting worse.

Thankfully, you can absolutely do something about your own password security, by following these Microsoft-endorsed best practices for enforcing password policies:

- **Enforce password history.** Set how frequently old passwords can be reused, if at all.
- **Maximum password age.** Preset how long users can keep a password before they have to change it. 30, 60, or 90 days are optimal values for small and medium-sized businesses.
- **Minimum password age.** Define how long users must keep a password before they can change it. This prevents users from bypassing the password system by entering a new password and then immediately changing it back to the old one.

- **Meet complexity requirements:**
  - Passwords must have at least six characters.
  - Passwords can't contain the user name or parts of the user's full name, such as first name.
  - Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.
- **Keep passwords in the password database encrypted.** Only enable the reversible encryption option on a per-user basis, only as required to meet the user's actual needs.

The above four "hands on" tactics will empower you to proactively protect your business from cybercrime in 2018. However, we encourage you to complement these measures with a robust, multi-tiered cybersecurity strategy and a dedicated IT Solutions partner like Fully Managed.

When it comes to protecting your data, there's no time like the present.

Call Fully Managed and secure your business today: **1.877.432.0747**