THE 12 DAYS OF CYBERSECURITY

daisy.

You're never too old to believe in cyberattacks. As December hits, the attentions of many businesses begin to divert away from PCs and processes and instead focus on digging deep into the abundance of cheer that surrounds them. But as festivities start to unfold, hackers are using this diversion as the perfect opportunity to dig deep into your business' data. Here we share 12 cybersecurity tips, best practice and advice that can be adopted now to help ward off any unwelcome visitors.

1. Always assume there is a vulnerability

Just because you have already invested time and money into a cybersecurity strategy does not mean your systems will be safe. There is always a new vulnerability to find or a potential flaw in the network or a new staff member to exploit. Always assume that there is a way for hackers to get in.

2. Leverage the cloud

The cloud is an incredibly useful tool, especially for smaller businesses that want to outsource the protection of their data to a larger company. That said, it is important to ensure that you have all the facts when signing up with a cloud provider. Ensure you know the location of their data centres and all the places they might be able to store and access your information.

3. Software updates

In May this year, the importance of software updates was brought well and truly into the spotlight, after Windows-powered PCs that weren't running the latest software were exploited and many businesses, including NHS hospitals, were left unable to access their systems. Software updates will frequently include patches for newly-discovered security vulnerabilities which cybercriminals are racing to exploit.

4. Use strong passwords

...and don't reuse them. If you are using the same password for every account then it won't be difficult for a hacker to gain access to all your systems. A hacker may often resort to 'brute force' to find your passwords, but this is much harder if the password is longer and does not spell out any words. Use a password manager of some kind to ensure you don't keep forgetting your passwords.

5. Password training for your workforce

Each of your employees should be trained on the use of passwords. Examples of such training would include: ensuring employees do not write passwords down (where they can be stolen); ensuring employees do not share passwords over any online communication; ensuring employees create strong passwords and use a company password manager; and ensuring employees do not reuse passwords for multiple company applications, or between personal and company use.

6. Establish a bring your own device (BYOD) policy

Many businesses now allow their employees to use their personal devices to conduct business. This is great for increasing productivity and efficiency but leaves businesses vulnerable to an attack since devices can be hacked and used to access your corporate network. A BYOD policy will help to educate employees on the use of mobile technology and how to mitigate the risk of an attack.

7. Understand what data your business is collecting

In order to keep your business' data safe, you should conduct an audit of all data and identify which data is public information (and therefore doesn't need to be closely guarded), which data has a medium importance and will not impact your business too much if discovered (this should have some security measures to protect it) and finally, which data is most important and personal to your business. The final category of data will impact your business greatly if lost or stolen and should be guarded safely with priority given to those with the most access rights from members of your business.

8. Secure your networks

Make sure your WiFi network is hidden and secure to avoid unauthorised access. You can achieve this by encrypting your wireless access point; disabling access from the outside network; and scanning your network regularly.

9. Keep a backup of all your data

Data backups ensure that in the event of any data loss or theft, files can be recovered. You should always backup your data in a different location so hackers cannot access both areas and you should also ensure backups occur on a regular basis.

10. Provide firewall security for your internet connection

Firewalls help in preventing unauthorised access from a private network. You can create a set of rules on your firewall so that it knows what to allow in and what to block out. A good firewall should monitor both incoming and outgoing data.

11. Conduct an internal threat analysis

An inside threat analysis will uncover any potential threats to your IT infrastructure that come from within your business. This could be anything from current or former employees to contractors, vendors, third party data suppliers or associates.

12. Form an incident response team

While having one person in charge of making sure an incident response plan is being followed, you will need a larger team to help that person follow through quickly. For example, a PR person to release any communications and a sales person to speak to customers. Depending on the size of your business and the size of the attack, you want to ensure the right people are managing the response.

Visit daisygroup.com/security to discover how Daisy can help your business stay secure at any time of year.

we are daisy.
www.daisygroup.com