IMPROVING YOUR STUDIO'S DATA SECURITY WELLNESS

MAKING YOUR HAIRDRESSING STUDIO SAFER

WHAT IS DATA ?

Data:

- Computer data is information processed or stored by a computer
- This information may be in the form of text documents, images, audio clips, software programs
- Data is collected through observation

Personal data:

- Is data that relates to an identifiable person.
- Some data and information that is stores is personal and must be kept private.
- Bank details, addresses, salaries, and so on, would be considered as a private and personal

WHICH DATA IS ON RISK ?

Personal data on risk:

- Name
- Address
- Bank details
- Phone numbers

Why keep it safe?

- The costumers and employees privacy
- The business public image
- Accomplish with the law
- Data breach cost money
- It is a good practice

FIREWALLS AND INTERNET GATEWAYS

FIRST STEP TO PROTECT YOUR BUSINESS

WHAT ARE THEY ?

Firewall:

- Can be hardware or software.
- Allow the connection if it is secure.
- Block unwanted traffic avoiding risks.

Internet gateway:

- It is a router.
- Key stopping point for data to go in or out from other networks.
- Filter between the business and internet.

KEY POINTS TO IMPROVE:

- Have all the information in one computer without a updatable copy.
- Use a USB flash drive to transport the sensible information.
- Very old operative system
- Share account on reception computer.
- Open Wi-Fi router where costumers and staff can connect connected to the rest of the network

SECURE CONFIGURATION

- Security measures that can be implement when installing computer and network.
- Prevent unnecessary cyber vulnerabilities and security misconfigurations.
- Security misconfigurations are one of the most common gaps that criminal hackers look to exploit.

IMPLEMENTING A SECURE CONFIGURATION:

- Default configurations are made to be as open and multi-functional as possible
- Accepting the default settings without reviewing them can create serious security issue.
- Failure to properly configure your servers and web services can lead to a wide variety of security problems.
- Computers and network devices with bad configurations could create vulnerabilities.

- Change default passwords
- Remove and disable unnecessary user accounts and control user privileges.
- Implement a password policy
- Disable any auto-run feature that allows file execution without user authorisation
- Disable unnecessary peripheral devices
- Update the systems and software always when patches are available.

ACCESS CONTROLS

WHO CAN MANAGE YOUR BUSINESS DATA ?

ACCESS CONTROL

What is it ?

- Method to guaranteeing that users are who they say they are.
- Gives the appropriate access to the company's data
- Gives to the users access just to the information that they need to get access to.

Why is relevant ?

- Minimize the security risk of unauthorized access to sensible data.
- Ensures access control policies are in place to protect confidential information.
- Without proper access control you could leave your company wide open to problems such as data loss.

WHERE TO IMPROVE ?

- Shared user profile.
- No privileges set up on users.
- No Strong passwords for costumers Wi-Fi.

- An user account and password per staff member.
- Every user has to have a privileges set up according to the information that they need to access, and no more.
- Implement a password policy in all the company including the public router can improve the general security.

MALWARE PROTECTION

Defend your network !

WHAT IS AN ANTI MALWARE ?

- Malware is the short of "malicious software". Which are computer programs design to infect computers.
- Malware can infect devices in several ways.
- Anti malware is a software that protects the computer from malware such as spyware, adware and worms.
- Scan the system for all types of malicious software that manage to reach the computer.
- Malware protection provides a second vital layer of protection for your computer or network.
- Robust malware protection specifically guards your finances

WHICH ANTI-MALWARE CHOOSE ?

Here a few options on different prices ranges:

Kaspersky

It offers one of the most reliable antimalware protection on the market.

Comes with some of the best anti-ransomware features.

Best option but the most expensive one

Price: £111 per year.

Emsisoft

Behaviour Blocker - a new tool against customized threats and new cyber-menaces

Dual virus and malware scanner (dual-engine)..

Anti-ransomware, Anti-phishing and PUP prevention.

The best budget option, can compete with the most expensive defensive software but for a affordable price.

Price: £ 43.59 per year

PATCH MANAGEMENT

PATCH MANAGEMENT:

What it is ?

- It is the process of distributing and applying updates to software.
- Patches are necessary to correct errors like vulnerabilities or bugs on the software and drivers.
- The manufactures release patches when they discover vulnerabilities

Why it is important ?

- Fix vulnerabilities on your software and applications that are susceptible to cyber-attacks.
- Help the software and applications run smoother.
- Most of the attacked business didn't have their systems update.

GOVERNMENT RECOMMENDATIONS:

WHAT THE GOVERNMENTAL ADVISES SHOULD KEEP ON MIND ?

ICO advices:

- Data protection laws applies to smalls business.
- The details of your customers and staff will be covered by the rules.
- When data protection goes wrong, it can also be costly.

GCHQ recommends:

- Use a strong and separate password for your email.
- Create strong passwords using three random words.
- Save your passwords in your browser.
- Turn on two-factor authentication (2FA).
- Update your devices.
- Back up your data.

WHAT THE GOVERNMENTAL ADVISES SHOULD KEEP ON MIND ?

Scottish government say:

- Cyber attackers increasingly understand that small business typically have more digital assets than an individual, but less security than a large corporation. Putting small businesses in cyber attackers' "sweet spot".
- Four in ten of all UK businesses suffered a cyber breach or attack in a 12 month period.
- Small businesses may face failure or bankruptcy as a result of ransomware attacks if they have not taken appropriate cyber security precautions.

Caroline, Your company is safe now !

ANY QUESTIONS

? ? ?