CYJAX

Website Security Is your website safe from cyber attack?

IT WON'T HAPPEN TO US

Did you know that the average cost of a cyber attack to a small business can run into thousands of pounds? Most companies haven't put contingency funds aside to deal with the rising costs associated with cyber attacks. Don't make the mistake of assuming your business is too small to be a target of cyber crime!

FIRST THINGS FIRST

Malicious software is constantly evolving and the only way to keep your systems protected is to ensure regular updates and patches are maintained. When systems are not up to date, they become vulnerable to attack. Is your network protected? Make sure you encrypt information, use firewalls and segregate networks.

HTTPS

All websites should use HTTPS; the "S" stands for secure. This ensures a secure, encrypted connection between the user's browser and the web server. It will help prevent intruders and malicious attackers.

PREPARE FOR ATTACK!

The two most common forms of attack against a website are XXS attacks and SQL Injections. Cross-site Scripting (XXS) injects malicious JavaScript into your website and allows a threat actor to make changes to your web pages. SQL injections are aimed at manipulating or destroying your databases. There are preventative measures you can put in place, with one being input validation, which will help protect you from both of these forms of attack. Ensure users can only input characters you have whitelisted; this will prevent them running bad characters or SQL statements.

PUBLIC ACCESS

It is a brilliant tool to have public access sections on your website for feedback or perhaps forums, but it is essential that unvalidated text or links cannot be posted in these areas, and that they are regularly monitored for phishing links and malicious comments that may damage your company's image.

PASSWORDS

Enforce a strong password policy across your organisation and ensure staff know not to write them down or share them with other staff members. If you store customer passwords, ensure they are encrypted at rest and in transmission to keep them secure. Consider two-factor authentication as an additional defence: this will make a hacker's job much harder. Administrator passwords should be changed more frequently and be more complex than standard user passwords.

PROTECT YOUR DATA

Is your Privacy Policy up to date? Since the General Data Protection Regulation (GDPR) came into force in May 2018, this is one of the most important documents your company has. It is the only way to demonstrate to authorities and your customers that you take data protection seriously. Every website must have a Privacy Notice, informing users of how your website will process and store their data. Ensure that a contact address is available for anyone who has any queries.

NO MEANS NO

Consent boxes must not be pre-ticked, as the customer must actively confirm their consent. Under GDPR, do not allow group consent with Terms and Conditions, privacy notices or any of your services.

IF YOU WOULD LIKE ANY FURTHER INFORMATION AND ADVICE ON CYBER SECURITY IN THE WORKPLACE, PLEASE CONTACT US AT INFO@CYJAX.COM OR VISIT OUR WEBSITE CYJAX.COM