Social Media in Modern Business

Expand Your Universe

Social media is a fantastic tool that businesses can use to market and promote products and services. One that allows you to become more visible online, communicate with your client base and nurture connections, whilst providing a cost effective way of sharing promotions and news. Nevertheless, it does so with risks of cyber attacks. Your social media presence opens a business up to everything from DDoS attacks to allowing the wrong person control of your feeds.

One of the biggest risks is your reputation, if you have an employee's personal page linked to your platforms or are sharing opinionated views that do not follow your ethos, missions and visions could give the wrong impression, be inaccurate or offensive to your clients and therefore could create disputes.

It's vital to remember that the moment you post, it's out there, even if you take the post down in seconds, screenshots can still circulate indefinitely.

Furthermore, there is a security risk associated with sensitive information under GDPR perhaps being sent via private or public messages and posts that could create data breaches. It is important to ensure the individual in charge of the business media accounts is dedicated to the marketing strategies in place and is given plenty of time and training to complete campaigns with skill, care and attention.

> "With GDPR setting out strict regulations over the capture, use and storage of customer data, and with the potential fine for non-compliance with the act being 4% of turn over, a small slip of the finger could cause big financial penalties for the business who makes one."
>
> (FSB 2021)

Social Engineering

Hackers may use social media as a way to contact staff, attempting to use social engineering to gain sensitive information regarding company and client data. Many emails will send links to try and deceive receivers that they are reputable, however, these attacks can infect the companies networks with malware which can cause a loss of data and/or breach, costing you time and money to cleanse.

Avoiding The Risks

In order to avoid the risks and protect yourself we recommend you have the following in place:

- A social media usage policy that is robust and provides a clear understanding of who can post.
- That employees are not recommended to add the workplace to their profiles. If they do, they must be
- educated in how their profiles and sensitive data is in the public domain.
- Limit access to those authorised to update platforms.
- Provide training on phishing and social engineering in order to spot suspicious behaviour.

Cyber Advice Line

Should you believe you have been a victim of a cyber attack, please check out Cyber Aware.

The National Cyber Security Centre support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public. When incidents do occur, they provide effective incident response to minimise harm to the UK, help with recovery, and learn lessons for the future.

Author: Kaitlyn Hogg | www.openbrolly.com

Openbrolly