BUSINESS IN THE COMMUNITY
The Prince's Responsible Business Network

HRH THE PRINCE OF WALES
ROYAL FOUNDING PATRON

Web presence for a small business

HOW TO WEAVE A SECURE WEB

A guide for business owners and IT managers

What is web presence?

Web presence is anywhere online that you or your business is represented. This could be through websites, social media or blogs. It is important to manage your web presence so that sensitive information does not come into the hands of a criminals, causing harm to you or your business.

What personal information should we include on our website?

Cyber-criminals will research their targets by gathering information about them posted on the internet. It is recommended that you monitor and restrict personal information included on your website and on social media. Adding employee biographies to your company website can be a nice touch but it is important to not overshare information including what town you are from, where you went to school or your favourite hobbies. With this information, attackers can build a picture of their target, enabling them to launch a social engineering attack.

Social engineering is when individuals are tricked into giving away personal information such as their password, usernames, bank details or mobile phone provider by criminals pretending to be someone else like your bank. Contained in the social engineering email would be a link to a website that looks like the bank's website but is fake and tricks you into entering in your login credentials. Another example would be an email pretending to be from someone that the individual knows, such as a colleague or family member, asking them to urgently transfer money into a bank.

How should we make our passwords strong?

It is important to use strong passwords for all online accounts. One way to create a strong password is to join three random words together. Numbers and special characters can also be added if required, for example Yell0wbeartree45! Use words that are memorable to you, but avoid using personal details that can be guessed by doing a quick social media search, such as: your partner's name, favourite sports team or the city you live in.

As well as using the three random words method, it is recommended to use a different password for each of your accounts. If a hacker does manage to gain access to one of your accounts, they could then access any other accounts where you use the same password. It can be difficult for a user to remember all the passwords to every account they use, at work and at home; this often leads to less secure practices such as re-using the same password.

Password managers are a helpful way to help you manage all your passwords. They are an affordable tool that help you create and store all your passwords. All passwords can then be accessed through a master password. There are many different password managers out there including 1password, Chrome, Keypass, Keychain and Lastpass. Please refer to the NCSC's Password managers buyer's guide for more information.

Even if you are using different passwords across all online services, they can still be compromised by criminals. For this reason, it is good practice to use Multi-factor Authentications (MFA). MFA, also called two-factor authentication (2FA), adds an extra level of security as it requires the user to provide an additional piece of evidence (factor) to sign in. Even if a cyber-criminal has access to a user's stolen password, they will still not be able to sign-in without the second piece of information. MFA can be used by organisations of all different sizes, as well as for personal use. Information on implementing MFA for organisations and personal accounts can be found on the NCSC's website.

How can we keep our social media secure?

Keeping your social media accounts safe is important so that you do not damage your business's reputation. The best way to do this is to have a social media policy that includes the following:

- Restrict the number of employees that have administrative access to your social media accounts to only those that really need to use it.
- Provide suitable training for employees.
- Set up an audit trail so that you can monitor who is posting and who has access to which accounts When an employee leaves the company immediately revoke their access.
- Monitor what is being posted about you, in your comments or on other accounts. Imposter accounts that look legitimate may have been created, posting inappropriate content.
- Monitor what is being posted on your account, if something looks suspicious it may indicate that someone has hacked into your account. It is worth investing in a social media monitoring tool such as Hootsuite or Keyhole: these allow you to monitor your presence across a number of different platforms saving you time.

How should we manage our third-party vendors?

Many companies are breached because of their third-party vendors' poor security. As part of your vendor screening process, investigate what security they have in place on your behalf. Hackers will often look for holes in a vendor's security to access a target's information. When you are vetting your vendor(s) there are several questions you should ask, for example: what cyber security training their employees have undertaken? Do they meet current data security standards?
If you are choosing a web hosting provider, look out for security add-ons such as domain privacy, SSL certificates and malware scanning tools. Reputable web hosting companies offer these add-ons and, while they may appear to do so at a slight premium compared to smaller web hosting companies, they have earned reputations as being reliable and responsive service providers. It is possible to reduce costs by hosting your own web presence on a virtual private server (VPS). However, the responsibility for patching, security and maintenance of the server falls under your remit. Finally, it is worth considering a managed web hosting package for an entirely 'hands-off' experience. Managed web hosting takes responsibility for everything about hosting, so you can concentrate on the design and content.

In Summary

Make sure you limit what you post on your website or social media, steering clear of any sort of sensitive information that could be used against you in a cyber-attack.

- Monitor your web presence by looking out for unusual activities on your accounts and posts from other accounts that could result in harm.
- Stay secure by only using long and complex passwords and make sure that you use a different password for each of your accounts.
- Ensure that any third-party providers have the relevant security protocols in place to keep your data safe.
- Stay informed on the latest risk by reading up on online forums discussing the latest risks, as well as websites to improve your general knowledge of cyber security such as the NCSC and Get Safe Online

COULD ALL YOUR HARD WORK BE HACKED DOWN TOMORROW?

BUSINESS IN THE COMMUNITY

The Prince's
Responsible
Business Network