How are you going to make sure both your business and your consumers are doing their utmost to protect yourselves against cyber crimes?

Research shows that businesses are in a conundrum. They aren't doing enough to protect themselves or their consumers, leaving them vulnerable to cyber attacks.

BSI has some top tips for both consumers and retailers:

Consumer Guide to Safer Shopping:

1. **Share only basic data:** When buying products online, only share the information needed to complete the purchase. Avoid giving your bank details away where possible or linking to your bank account details with payment tools.
2. **Stick to trusted websites:** Always shop around for the retailers with the best reputations. Symbols such as the Secure Digital Transactions BSI Kitemark™ or the closed padlock symbol at checkout, guarantee that the retailer meets industry-required security standards. The padlock symbol on your web browser's address bar and URL addresses that begin with 'shttp' or 'https' also indicate secure sites and that your data is encrypted.
3. **Beware of phishing scams:** Be wary of emails asking for your personal details, even if they appear to come from your bank or service provider. If you're unsure, check with the real business first.
4. **Use your card but don't let the site store your details:** The fewer sites that have your data on file, the better. The easiest way to do this is to uncheck the 'Don't store my card details' option at checkout. Other tools such as MasterPass can also help keep your data secure.
5. **Keep software updated:** Do regular checks for upgrades to your operating system or software updates and install these. Making sure you have the latest patches for anti-spyware and anti-virus programs are also a must, as these will ensure nobody can track your internet use or infect your device.
6. **Beware public computers and public Wi-Fi:** When using a public computer, always log out and close the browser when you're finished. If you're given the option of free Wi-Fi, avoid giving personal or payment information and choose to browse using the 'Public browsing' setting where available.
7. **Be cautious in responding to emails:** Think twice before responding to an email from someone you don't recognise or an email that seems out of character. These are common phishing tactics, so if unsure then do not respond or click links in the email or click on any links.
8. **Diligent downloading:** Only download from sites you know and trust and ensure that you have the highest levels of security on your downloads, to prevent any malware accessing your computer whilst browsing.
9. **Keep records:** Regularly review your bank and credit card statements for unusual activity. This could indicate that your account has been hacked and would require to you to contact your provider to have your details changed. Always keep electronic receipts as backup.
10. **Always look for the tick box:** Many companies automatically will opt you in to receiving marketing emails, newsletters or to pass on your detail to third parties. If you don't want this, make sure you uncheck or check the relevant box during the buying process.

bsi.

...making excellence a habit™

Retailer resolutions:

1. **Guarantee security:** Give consumers confidence by guaranteeing security of data when entering personal details. Symbols such as the Secure Digital Transactions Kitemark, The Cyber Essentials logo or the closed padlock symbol are looked for by consumers as confirmation of that site's security when making online purchases.
2. **Avoid sharing data with third parties:** One of consumer's major bugbears with online retailers is having their details shared with third parties, as shown by recent BSI research. Opt consumers out of receiving third party information by default to encourage them to shop with you.
3. **Don't sell on data:** In addition to restricting third party marketing materials, ensure that customers can be confident that their data will not be sold on without express permission.
4. **Keep hardware up to date:** Ensure legacy IT equipment and systems are updated to a secure standard.
5. **Use the latest software**: Ensure software running on computers and network devices is kept up-to-date.
6. **Ensure your staff know how to keep data safe:** Set up an internal information security policy to follow and appropriate staff training. **75% of large organizations and 31% of small businesses suffered staff-related security breaches in the last 12 months, with 50% of the worst breaches caused by inadvertent human error.**
   Source: HMG, 2015 Information Security Breaches Survey
7. **Install anti-virus software:** Protect yourself when online and from mobile devices with comprehensive anti-virus software.
8. **Control employee access:** Keep records of users' access to applications, computers and networks.
9. **Use secure cloud based services with care:** The cheapest cloud storage services aren't always the most secure – ensure that any cloud storing personal or confidential information has appropriate security measures in place.
10. **Regularly refresh passwords:** Change passwords regularly to avoid hacking of personal data or misuse by rogue employees.

There is no one solution or silver bullet for cyber security, but BSI can help your organization wherever you are on your information security journey.

Contact us now to see how we can help you: +852 3149 3300

bsi.

Speak to one of our experts today or visit our website for more information.

Call: +852 3149 3300
or visit: bsigroup.com/en-HK