Tip of the Month – December, 2012

Christmas Privacy Tips

Here are some seasonal privacy tips on how to keep your personal details safe over the holiday period.

- When shopping on-line, you can limit the risk of someone stealing your credit card details and racking up huge purchases by having a separate, low-limit credit card.

- Make sure you've got up-to-date safety software on your computer, especially if you are banking online.

- Use a nickname instead of your own name on social networking sites.

- If you want your on-line profile to be seen only by registered friends, ensure the profile setting is not on ‘open access'.

- If you are planning a New Year's Eve party, invite friends directly by email or phone rather than advertise it on a Facebook or MySpace page.

- If you use a computer at an internet café, make sure you log off before you leave - if not, anyone could access your account.

- Be careful with any personal information you are throwing away at Christmas time such as bills and letters. Shred, burn or destroy them.

- Think before you give out personal information and ask what it will be used for - for example, check with retailers before you sign up to competitions or for promotional information.

- While you are on holiday, secure your personal information left at home such as National Insurance Card and personal documents, and information you take with you such as your drivers licence, or credit cards, or on laptops.

- Keep an eye on your wallet, cell phone, smart phone or laptop, for example, especially in busy shops, bars and holiday spots. Don't leave them unattended - thieves could have a field day with your information.

- Remove unnecessary credit cards or documents from your wallet or bag that could compromise your identity if you lose them. Don't keep nonessential details on your cell phone - do you need everyone's addresses and extra details on your phone? The more personal information an identity thief can get hold of, the easier their job becomes.

- Don't advertise on social networking sites that you will be away. This would be like putting a sign on your front door that says "I'm on holiday - burgle me!"

- When shopping online, only send personal or financial information using a secure transaction system, usually shown as a website address that begins with https://

- Check out a website's privacy policy before providing any personal information.

- After the holidays, check your credit and bank statements as soon as they arrive so that anything that doesn't look like your spending can be reported straight away.
- Be aware that some links in emails can take you to websites with malicious content, which could result in your information being used fraudulently. Before you click on a link, look at exactly where it will take you by running your mouse over the link to show the URL. If you are not certain that the website is legitimate and safe, do not click on the link. It's safer to type the URL into your internet browser.
- Don't give your details online to anyone you are not sure about. Even an email seemingly from a friend asking for your information or help could be malicious. Be certain you know who you are replying to - check that the return address is correct. If it's not and you reply, you could be replying to a scammer.
- Be wary about downloading holiday ringtones, Christmas carol lyrics or festive screensavers. They could infect your computer with spy or malware. Check that your own computer is secure with up-to-date firewall, anti-virus and anti-spyware protections.
- If using the internet in a cyber cafe or other public place, don't access or send sensitive information such as your banking details. Public computers are prime targets for hackers. Also, public internet services won't necessarily be encrypted, so your information on them may not be secure. Make sure you log off all your accounts before you leave.
- SMS-Spoofing, or sending fake texts, is increasing. Via the internet, someone can alter their identity so that a text appears to be from someone else such as a relative, your boss, or a company. Be cautious about replying to texts that ask for any personal details - make sure you are confident you know who is asking for your information, though it's much safer not to reply at all. A text might appear to be from your bank or a friend when in fact it's from a cyber-criminal.

- When using Wi-Fi, make sure you use at least https - the secure version of http. Https provides encryption and creates a reasonably secure channel over the internet, safeguarding your communications from cyber-spies or attacks. Also, use secure Wi-Fi hotspots for more confidence that your information will not be compromised.

Enjoy your holiday and stay safe!

For more information on this and any other data protection concern you may have, please email us at dataprotection@bahamas.gov.bs or visit our website www.bahamas.gov.bs/dataprotection.

Remember "Privacy is the Best Policy"

(Adapted from the Privacy Commissioner of New Zealand)