

Tip of the Month - December 2011

Protect your Privacy this Christmas

Bahamians are becoming more sophisticated and many will be doing more shopping online this year. You should know therefore that Cyber-crooks are also gearing up for the holidays so you should stay alert against fraudsters who will make merry with your online personal information. You should therefore note the following tips:

- Research your merchant – look at customer ratings, and the merchant’s privacy and security policy.
- Reputable merchants usually send you an e-mail confirming your order.
- Use a low limit credit card for online purchases and one that provides you with specific guarantees, such as 100% coverage for any losses due to fraud when shopping on the web.
- Watch for spyware, adware, or other internet attacks as you conduct online transactions.
- Don’t use the same username and password at every website. If your personal information is compromised, a thief will not get very far if you use different passwords and usernames on different websites.
- Never share your website passwords and online banking account information with anyone.
- If a product or service looks too good to be true, it probably is.
- When asked for your personal information such as your name, address, telephone number, ask the store merchant why she is collecting it and how it will be used.
- Keep your credit card receipts to check against your monthly credit card statement.
- Shred sales receipts, and other paper that displays your credit/debit card or bank account numbers – thieves are known to sort through residential trash to find these items which may be used to commit identity fraud.

- Beware of slick professional – looking phishing emails or malware which try to get you to disclose your financial and personal information.
- Don't give your PIN to anyone or write the number down (e.g. on your debit card).
- Don't leave purses or wallets in your vehicle, or unattended in a store.
- Don't carry your NIB card or Passport in your wallet or briefcase.
- Cover the pin pad with your hand when entering your PIN into a debit card machine or ATM.
- Keep an eye on your credit card when you give it to the store clerk or waiter – make sure it's not out of your sight.
- If you see something suspicious relating to point of sale terminals or ATMs, report it to the store merchant.

Tips for Merchants

Retailers are reminded that they also have certain obligations under the Data Protection (Privacy of Personal Information) Act, 2003 (DPA) to protect customer and employee information.

- Don't collect information if you don't need it.
- For fraud prevention purposes, you may ask to see proof of identity when a customer pays with a credit card, but it is not reasonable to record the driver's licence number or photocopy the ID.
- Only employees who "need-to-know" should have access to personal information.
- Make sure that credit card numbers are properly obscured or truncated by point of sale terminals.
- Point of sale terminals should be visible to customers: credit and debit cards should not disappear under the counter to be swiped.
- Know how your point of sale terminal operates – do you know if the hard drive collects and store customer credit and debit card information?

- Protect your personal information – store paper records securely; ensure information on your computers is protected with adequate safeguards, such as passwords; shred or securely dispose of all customer information once it is no longer needed.
- Train and retrain staff about your refund policy so they can explain to customers why you collect customer personal information and how it will be used.

HAPPY HOLIDAYS!

Remember “Privacy is the Best Policy.”

Feel free to contact us at, dataprotection@bahamas.gov.bs or visit our website www.bahamas.gov.bs/dataprotection to learn more about our mandate to protect the privacy rights of individuals.