

reallife

CARIBBEAN LUXURY LIFESTYLE, PROPERTY AND DESIGN MAGAZINE

in this issue

- Beyond Electric Avenue – Eddy Grant
- Caribbean Market Trends
- Company Profiles – IDG, Oasis Pool & Spa, OtisAir and Trio Architecture
- Caribbean Resorts – Above All Expectations
- Artist – Vivacious and Vibrant, Vanita

EXCLUSIVE SHOWCASE PROPERTIES

CASA DEL CIELO

A FAMILY HOME IN CAYMAN OPENS ITS ROOF TO THE SKY

VILLA UTOPIC

MODERN ARCHITECTURE MEETS
CARIBBEAN COLOUR IN ST. BARTHS

VILLA MANGO

A SOPHISTICATED YET PLAYFUL ABODE IN CAYMAN



FEATURE PROPERTIES IN CAYMAN

ARVIA

LUXURY CANAL FRONT LIVING MADE EASY

THE RESIDENCES AT SEAFIRE

WHERE STYLE MEETS SUSTAINABILITY

THE RESIDENCES OF STONE ISLAND

PRESTIGIOUS WATERFRONT LIVING ON A PRIVATE PENINSULA



STAY SECURE

Words by Aneal Sobie, Manager - Information Security at Cayman National Bank Ltd.

There's no doubt the Internet has changed the way we live, but the convenience of all this connectivity doesn't come without risk. Cybercrime is an ever-present threat and it's essential to take some basic precautions to safeguard your personal data. Steps you can take to improve your online security include:

SECURE PASSWORDS

Make sure your passwords are strong. Dictionary words or the names of a loved one are not secure. Recommended practices include:

Using a passphrase: this involves choosing a phrase which is easy to remember, condensing it and swapping out some letters for special characters.

Avoiding using the same password for different websites and apps: password managers can help keep track of your credentials.

Using multi-factor authentication: this combines the password requirement with a biometric such as a fingerprint or a one-time code that is generated on your device or sent via SMS/email.

UPDATE DEVICES

Keeping your devices updated is a vital part of being secure. It's also important to reboot at least once a week. New vulnerabilities are continuously being discovered and may be exploited. This also applies to any third party software such as Adobe or Java.

It is imperative to also update your Anti-Malware and run scans on a regular basis for it to be effective. There are several free Anti-Malware programs available or you can sign up for a premium version which may have additional features.

Free Anti-Malware programs available which can be of use are: *Bitdefender Antivirus Free Edition* (www.bitdefender.com), *AVG Antivirus Free* (www.avg.com) and *Malwarebytes Anti-Malware* (www.malwarebytes.com).

BEWARE PHISHERS

Social engineering is a major online threat, which is mainly done via phishing emails and

links. These appear to be a legitimate request for information, but your details are then harvested and sold or used in an attack. If you receive an email you suspect to be a phishing scam, one response is to contact the sending organisation directly (do not reply to the original email) and verify the legitimacy of the request.

BACKUP YOUR DATA

To avoid losing any critical data (photos, documents, music) back up regularly. If you do suffer a data loss, a recent viable backup can be a lifesaver. Backups can be done to the cloud or to an external hard drive. Several cloud services offer backup services, and these can provide redundancy but will require an Internet connection to access your data. An external hard drive can be useful if the Internet isn't available, but be sure to encrypt your data.

SECURE WI-FI

Leaving your Wi-Fi open can expose your devices to attack. This isn't limited to laptops and phones, many appliances now connect to the Internet and can be exploited or used to launch attacks against others. Your Wi-Fi should be secured by using a strong passphrase and controlling which devices are allowed to connect.

MONITOR YOUR ACCOUNTS

Detection and prevention go hand in hand, and the earlier you can identify if an online account has been compromised, the more likely it is that you can limit or prevent fraudulent or malicious activity. Make it a habit to review your bank and credit card statements for any suspicious transactions. Some banks offer a transaction notification service which can alert you if your card details have been used for a purchase or ATM withdrawal. Similarly, there are online notification services, e.g. from Google, which can alert you if they see a login from a new device or IP address. These can be important indicators of compromise and should be heeded.

WHAT TO DO AFTER A COMPROMISE

Despite our best efforts we may still fall victim to an attacker and have to take steps to limit or remediate the potential damage. There are several steps you can take if this occurs:

Change your passwords: If you discover an account is compromised, you should at the very least change the password for that account. However, our online identities are so linked, it would be advisable to change all of your passwords.

Email especially can be used for this, we often have an email address set for password recovery, if that email is compromised, your passwords can be reset and access to your accounts can be gained by the attacker.

File a police report: If you believe your identity or card information has been compromised, contact the local police, whether here in Cayman or if travelling abroad. This is a crime and you should alert law enforcement, as you may need a report when informing your financial institutions of the compromise.

Contact your financial institutions: You should alert your banks and other financial institutions that your account has been compromised and there may be the possibility of fraudulent transactions. You may want to go as far as putting a freeze on your cards (if your details have been stolen) to prevent their misuse. At the very least you can ask that they closely monitor your account for unusual transactions.

These steps can help improve your online security, making it more difficult for a successful attack. However, they are most effective when working together, as attackers will use several methods for gaining access. While no system is ever 100% secure, by improving your security you may deter an attacker from targeting you. 

For more information contact Cayman National:

Call: 345.949.4655

Visit: www.caymannational.com