SAFEGUARD SECURITY (PVT) LTD
A member of Safeguard Security Group
Branches Nationwide
36 Telford Road, Graniteside, Harare P O Box 66006 Kopje
Telephone 751395-9, 771084 (all hours) Fax: 770351
Email: info@safeguard.co.zw
Website: www.safeguard.co.zw

QUALITY CERTIFIED

5 June 2018

Company

Our office in Mount Pleasant is fully established now at **24 Coull Drive. We have a great team there headed by Wayne Du Plessis.** The office is open for you 0730 to 1700 Monday to Friday for enquiries, payments, and advice. Please do not hesitate to contact our team directly for assistance – we have included their details at the bottom of this report

We have included a bit of advice from Russell Magaya on the importance of strong password. Russell is a very well qualified **Cyber Security Practitioner**, and is available for advice and assistance in this area as needed.

BREAK IN REPORT – MAY 2018

1/5/18 at 07:14 hrs our client from City Centre telephoned our control room advising us of a break in the night before. Intruders gained access through the roof and stole float money. The alarm did activate the night before and sent numerous signals. The Client was advised to come and open the shop and check inside with the Response Team as this is normally a sign of an incident. The team did not see any sign of a break in from the outside. The Client declined to come as he suspected rats to be causing the false alarms.

On 2/5/18 at 01:09 hrs an alarm signal was received from the city centre. Intruders gained entry by opening the main shutter door using a remote button which was supposed to be with the client. **The alarm triggered and they ran away.** Police are investigating this mystery as to how the intruders had access to the remote.

On 2/5/18 at 21:21 hrs an alarm signal was received from the city centre. Intruders gained entry through the roof and stole some money from a cash box. **The alarm triggered and they ran away.**

On 3/5/18 at 01:16 hrs an alarm signal was received from a base station in Tafara. Intruders gained entry by using a log to break the palisade bar but **fled empty handed when the alarm sounded**.

On 3/5/18 the control room was alerted of a break in from Norton. Intruders gained entry by cutting the razor wire and climbed through the roof where they cut the alarm wires hence **no signal was received as the alarm system was unarmed.**

On 6/5/18 our client from Borrowdale phoned the control room to advise us of a break in the night before. Intruders gained entry by cutting the razor wire and breaking the burglar bars. **Alarm system was unarmed as it was faulty.**

On 7/5/18 at 02:36 hrs an alarm signal was received from the city centre. **On arrival the response team spotted an intruder inside the shop who they arrested and handed over to central police station.**

On 15/5/18 at 22:13 hrs an alarm signal was received from Hillside. Intruders gained entry by breaking one of the reception windows but fled empty handed when the alarm sounded.

On 16/5/18 at 02:11 hrs a panic signal was received from the city centre. Intruders gained entry by cutting the screen mesh wire and forced open the front door. They vandalised the alarm keypad and sensors. **The response team arrested one of the intruders and recovered the client's property.**

On 22/5/18 at 01:15 hrs an alarm signal was received from Eastlea. Intruders gained entry by forcing the reception door and breaking the lock but **fled empty handed when the alarm sounded.**

On 23/5/18 at 21:32 hrs an alarm signal was received from the city centre. Intruders gained entry by breaking the locks but **fled empty handed when the alarm sounded**.

On 26/5/18 our client from Mbare alerted us of a break in the night before. Intruders gained entry by jumping over the razor wired durawall and tried to force open the door to his instrument room, he heard the noise, woke up and they ran away. **The alarm system did not sound as it was not armed.**

On 27/5/18 our client from Mandara alerted us of a break in the night before. Intruders broke into three vehicles - **this area is not covered by the alarm system, and the system was unarmed the night before.**

MIDLANDS PROVINCE

Masvingo

On the 30/5/2018 at about 23:58 hrs in Zimre Park intruders cut the razor wire and jumped over the pre-cast wall. While inside the yard they then forced open the kitchen door **and the alarm went off waking up the owner** and the intruders ran away. Reaction team quickly responded and upon checking the premises with the owner of the house they found out that nothing had been stolen.

BULAWAYO

On 16/5/18 at 04:55hrs an alarm activated at a city butchery and our response arrived within 5 minutes and found the main door open and locks broken. The Key holder was contacted and on it was found that a 22 inch Plasma TV had been stolen. The TV was not secured to the wall and it is suspected the intruders grabbed what they could see and ran off when the alarm sounded.

On 7/5/18 at 08:00 hrs we received a call that some property had been stolen from the yard of an Engineering Company. The alarm did not activate as the area where the property was, **has no Alarm coverage.** The property stolen was 4x 25 litres of concrete curing agent and recommendations were made to install out door sensors to protect the area where stock is left at night.

On 10/5/17 at 07:00 hours we received a report that a Night club had been broken into. **The alarm which was installed by a third party did not activate for reasons unknown** and intruders smashed a glass door and stole whisky and a television set. Recommendations were given to install security lights, external beams and to ensure that the alarm is serviced and checked by a qualified technician.

On 24/5/18 at 03:30 hours an Electrical Hardware shop was broken into through the roof. **We had installed a sensor in the roof and the alarm activated and the response team was on site within 4 minutes.** The intruders fled the scene without gaining entry or taking anything from the client.

On 30/5/18 at 05:00hrs an alarm activated at a local Café. The intruders opened a small window and gained access to the premises before taking a cash box left with a float and left the premises before the response team arrived. The window is left open to allow a cat into the premises.

MUTARE

On the 23/5/18 we received a phone call from one of our clients requesting for our attention. We attended and noted that intruders had broken into the client's house the previous night. The client has a panic system. The break in was only noticed in the morning and the client called us. Nothing was reported stolen.

On the 22/05/18 at 23:52 hours we received a panic signal from one of our clients. Our response vehicle was dispatched and on arrival they met a petrol attendant who advised that he was robbed 287.84 litres of fuel. The petrol attendant advised that he was forced to fill fuel in containers which the robbers had. After filling they sped off in a Honda fit vehicle without registration number. The accused people are said to have been armed with machetes and knob carries.

SAFEGUARD BREAK-IN REPORT MAY 2018

We enjoy bringing you the latest security news, exclusive offers and break in reports. If you do not wish to receive these emails (including special offers) you can unsubscribe here or reply to this email clearly stating UNSUBSCIBE in the subject.

Coull Drive contact details

Wayne Du Plessis, General Manager Diploma cell phone 0772 235 048
Email: dipmanager@safeguard.co.zw
Patrick Masunga, Residential Manager West cell phone 0772 542 187
Email: guards2@safeguard.co.zw
Jonathan Tsikai, Residential Manager East cell phone 0773 198 548
Email: guards2@safeguard.co.zw
Or our Main Reception at 24 Coull Drive: +263 4 301765

Monthly Cyber Security Advice Newsletter May 2018

from the Desk of Russel T. Magaya

Why use secure passwords

How secure is your password?

Passwords protect our computer systems and data from falling into the wrong hands. Unfortunately, many users still use weak passwords. According to Verizon, 63% of data breaches involve use of weak, default or stolen passwords. Splash Data's annual list report of the worst passwords also show that people continue to use 'easy -to-guess' passwords to protect their information.

Malicious actors such as hackers rely human instincts to narrow down possibilities and guess passwords. Hackers are aware that users prefer easy to remember common words over long complicated passwords. Just tweaking an easily guessable password i.e. adding extra digits or replacing letters with a number or symbol – 'password' to 'p@ssw0rd' - , does not make the password stronger.

According to a security expert Bruce Schneier:

“Crackers use different dictionaries: english words, names, foreign words, phonetic patterns and so on for roots; two digits, dates, single symbols and so on for appendages. They run the dictionaries with various capitalizations and common substitutions: "$" for "s", "@" for "a", "1” for "l" and so on. This guessing strategy quickly breaks about two-thirds of all passwords.”

Each year SplashData compiles a list of commonly used bad passwords which are scrapped from stolen credentials leaked by hackers. Some of the examples are shown below for 2018 in comparison to 2017:

You can access the current full list of top 100 popular worst passwords HERE

Recommendations

How to Create Secure Passwords:

Always choose strength over convenience when selecting passwords.

Users are recommended to use strong and unique passwords which are not easy to guess. A strong password consists of at least **8 characters and includes a combination of uppercase and lowercase letters, numbers and symbols.** A unique password is one that is used with only one account.

- Do not use names, places and dictionary words regardless of language or personal information that someone might know or can easily obtain. They are the first ones hackers will try to gain access to your accounts. Also avoid using pin ‘1234’ on bank cards
- Change passwords regularly at least every 60 days. Avoid merely adding a number to the old password and avoid password reuse.
- Use different passwords for each of your account and make sure your work passwords are different from your personal passwords.
- Change router and system default passwords such as admin.

Protecting your passwords:

- Do NOT write down your passwords.
- Do NOT share passwords or pins with anyone.
- Do NOT provide login details in emails or over the phone to anyone even to your bank.
- Always remember to logout before leaving your desk.
- Follow your organisation’s password policies.

There is good technique suggested by Bruce Schneier in 2008 and also recommended by the Centre for Internet Security to assist in building strong, unique passwords. It involves to choosing a repeatable pattern for your password,

such as choosing a sentence that incorporates something unique about the website or account, and then using the first letter of each word as your password. For example, the sentence: "This is my January password for the Center for Internet Security website." would become "TimJp4tCfISw." This password capitalizes 5 letters within the sentence, swaps the word "for" to the number "4," and adds the period to include a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern. Variations on this technique include using the first letters from a line in a favourite song or a poem.

Resources for more information:

Connect Safely: Tips for Strong, Secure Passwords & Other Authentication Tools: http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/

Techadvisor: How to Create a Strong Password - and Remember it: https://www.techadvisor.co.uk/how-to/internet/create-strong-password-3357177/

Webroot: How Do I Create a Strong and Unique Password?: https://www.webroot.com/us/en/resources/tips-articles/how-do-i-create-a-strong-password

To check how secure is your password follow this link: https://howsecureismypassword.net/

The information provided in the Monthly Security Advice Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment and also at home.

About the author: Russel Magaya is an IT security professional currently studying for a Doctorate in Cybersecurity at Oxford. Russel is the Director of Izwi Technologies, a firm that provides IT solutions to businesses which include Cyber security services such as network security audit and implementation; policy formulation, compliance and governance; risk assessments; as well as Cybersecurity education, training and awareness. Contact detail: rtmagaya@gmail.com