Caution needed with online purchasing as Christmas approaches

By Richard Keymer

13 Oct 2014

As with other types of crime, incidences of banking card fraud tend to increase over the festive season. While there is ongoing coverage in the media of the various scams taking place locally and internationally, many consumers are still at a loss as to the various methods hackers may use to gain access to confidential banking information, and how best to keep their personal information safe online.

© olly - Fotolia.com

At a high level, the three most common ways hackers gain access to confidential information in the South African context is via phishing, SIM card swaps and in a few incidences, Trojan Horses.

Phishing

Phishing remains the most common way that many South Africans continue to disclose their personal information online erroneously. This is where fraudsters pose as a financial institution and circulate an email that looks like it comes from an official site such as your bank, but it comes from an external party, masquerading as the financial organisation.

Usually the email will ask you to visit a site, or provide some information, which looks very official and proper, except that the site is not what you think and the information that you give them allows them to steal your online identity and banking details.

SIM card cloning

When it comes to SIM card cloning, fraudsters exploit various different weaknesses in the system to enable the SIM swap process. In addition, while two factor authentications do reduce instances of this type of fraud, unfortunately, it does still happen.

Here the person will get hold of someone's Internet banking details, usually through a phishing attack and set up banking account/s to which money can be transferred and withdrawn. Once the SIM card has been cloned, the fraudster will create beneficiaries and transfer money to these beneficiaries, finally withdrawing the money from these accounts. Because SIM swap fraud usually works hand-in-hand with phishing, users should apply the same protection mechanisms.

Trojan Horses

While Trojan Horses are not that common in South Africa, instances of Trojans, specifically Zeus and Kronos, did affect the local market.

Trojans pose as innocent programmes but are designed to steal computer users' private data. These Trojans tend to be compatible with all major browsers such as Internet Explorer, Mozilla Firefox and Google Chrome and are able record all information that the users enter into their browser, including bank account details.

To do this Trojans make use of web injects to alter legitimate banking web pages. Once the user logs into his or her account, the web injects look for data about the user, generally searching for information that is required to answer security questions. When the malware acquires that data, the Trojan horse sends it to a remote server where it can be used by the cyber criminals.

Top tips

With these threats still prevalent within the local market, top tips for keeping personal information secure online include:

1. Ensure you download the latest banking apps directly from the official websites of the financial institutions or from reputable online stores. The official apps will have built-in security mechanisms.
2. Beware of using Wi-Fi hot spots in hotels or restaurants. If you are travelling and using internet hotspots or free Wi-Fi, extra precautions must be taken. Rather use 3G or trusted infrastructure when using banking apps in these environments.
3. Ensure your username and password are unique to the banking site and change these regularly. Never provide your online ID, password or PIN to anyone and never write them down or save them on your desktop. Also, do not make passwords too personal. Preferably, create passwords that have letters, numbers and symbols in them that cannot be attributed to you.
4. Do not ignore SMS or emails from the bank but also be wary of using contact details supplied. Rather go directly to the website or independently look up number. Also, do not open attachments or click on links in emails. Always bear in mind that no bank will ever ask you to confirm or update account details via e-mail, SMS or telephone.
5. Keep antivirus software and patches up to date. Many virus infections need not occur. Software vulnerabilities that malware exploits often already have fixes available by the time the virus reaches a computer. It is thus essential that the user install the latest updates that could have prevented these infections in the first place.
6. Be vigilant regarding your mobile phone's network connectivity status. If you realise you are not receiving any calls or SMS notifications, something may be wrong and you should make enquiries to be sure you have not fallen victim to a card swapping scam.

Internet users need to actively educate themselves and keep up to date with the latest online scams. Fraudsters are always on the lookout for new and clever ways to prey on the unsuspecting public when it comes to gaining access to your confidential online information.

It is important to be alert and share information regarding any possible scams. Ultimately it's always advisable to be overly cautious when it comes to using banking apps or disclosing confidential information.

ABOUT THE AUTHOR

Richard Keymer is the Head of Pre-sales at SecureData Africa.