BIZCOMMUNITY

Card, cybercrime threats to look out for this festive season

By Hein Kern

7 Dec 2016

Consumers are eager to spend and retailers are keen for the windfall of the holidays but when people are more spendthrift, criminals are more alert. This is particularly true for cybercriminals, cashing in on the holiday spirit.

Digital retail channels have grown tremendously, with over 45% or retail transaction volumes already originating from mobile devices. Fraudsters target this, which is why over 60% of new fraudulent activities also happen via mobile transactions.

(c) Worawee Meepian - 123RF.com

Credit, cheque and debit cards are targeted as well, not the least because they are often used in online transactions. It can be tricky for retailers to detect and pursue such crimes, says Hein Kern, territory manager for RSA Southern Africa, “Seventy percent of retailers take several days to investigate fraudulent activities on their websites, if not longer. This means criminals can do considerable damage to earnings before a retailer has caught on, with losses waiting down the line to dampen the holiday sales boost.”

Card crime trends

Several trends assert themselves over the holiday period, ones that retailers should be aware of to keep an eye out for fraudsters. Kern explains why there is a jump in card crime:

- Underground marketplaces for cloned and stolen cards ramp up activities, since they know the window to sell and exploit stolen card information closes fast. This results in a higher demand, so card-theft and cloning increases. As a result, there are a higher number of cloned cards in circulation, as fraudsters seek to exploit stolen card information.

- Due to limited protection in the global EMV (EuroPay, Mastercard and Visa) card standards around ‘card not present’ transactions, outlets that do not require a physical card, such as online and telephonic retail, become easy targets.

- Retailers whose card readers are not implementing EMV standards properly are also targets for criminals, who can inject false information in transactions and make them seem legit.

- Consumers are targeted more frequently with phishing attacks, namely fake emails, messages and websites that aim to steal their personal data. Criminals then use this information to apply for legitimate banking cards using stolen credentials.

- Criminals attempt to install malware and other dangerous software on consumer devices by infiltrating retail sites and using them to infect visitors.

  If these threats seem unlikely, consider how much of your retail transactions are done using banking cards. While traditional fears around criminality surround cash, it is easier to detect questionable activities or losses. Card systems are more opaque and the results of a theft may not be apparent if not monitored.

Protective steps for retailers

Fortunately, retailers can be proactive and prevent many of the problems:

- Ensure that card readers are up to date and support the latest EMV standards properly

- Request proof of identification when presented with a card for a transaction

- Speak to your financial institution about insurance, responsibilities and remedial action if fraud does occur.

- Train staff to understand and anticipate card fraud activities

- Partner with a security technology firm such as RSA and see which solutions can help detect and prevent fraud

- Audit your website’s security standards and policies and have detection in place to catch site infections and hijacking

- Educate your customers about keeping their cards and personal data safe

- Maintain an easy way for customers to contact you to verify correspondence from your company and alert you of any fraudulent activity

“The bad news is that if you think you can just ignore this, you will be a victim. Technology fraudsters are becoming better and faster but the real weak link is us. When companies and consumers do not pay attention to these threats, we create an opening for criminals. However, if we are vigilant and smart, they will look for easier targets instead,” concludes Kern.

ABOUT HEIN KERN

Hein Kern is territory manager at RSA Southern Africa, the security division of Dell EMC.
- Card, cybercrime threats to look out for this festive season - 7 Dec 2016

View my profile and articles...