By Ingrid Beierly

VULNERABILITY

Avoid Giving Credits When None are Deserved

A debit card was recently credited with several thousand dollars for returned merchandise, per the instructions from the merchant account holder. Does that sound pretty routine to you?

Award yourself a point if you guessed that this transaction was bogus (even if the title gave it away). In fact, no goods were ever sold in the first place, and as it turns out, the debit card in question actually belongs to a criminal operating from another country.

The means by which the thief was able to pull off this particular heist illustrates the resurgence of an old fraud scheme. Here's how it works: A criminal uses phishing, voice phishing (vishing) or other deceptive social engineering tricks to target merchants, using weak authentication to their payment gateways or processors. A variation of phishing known as spear phishing is specifically directed at high-profile targets within businesses. These attacks frequently reference names and personal information familiar to the target (often drawing from information gleaned from social networking sites). Fraudsters will also use another form of phishing scheme called drive-by downloads to install a key logger on a merchant's system. Drive-by downloads may happen when visiting a website, viewing an email message or by clicking on a deceptive pop-up window.

The goal is to obtain access to a Web portal of the merchant's payment gateway or processor. Using stolen merchant credentials, merchant ID and terminal ID, fraudsters are sending fraudulent credits to debit cards that they or their associates have set up and subsequently are performing ATM withdrawals.

In some cases, a criminal will even go so far as to send bogus sales transactions with offsetting debits. That way, he increases the chances that the order will avoid further scrutiny and decreases the odds of detection prior to the transaction's completion. Thus, it appears as if a credit for returned merchandise has been applied to a customer's debit card.

Using phishing and other deceptive tricks, criminals obtain access to a Web portal of the merchant's payment gateways or processor and send fraudulent credits to debit cards that they have set up.

Any hotel or restaurant operator using weak authentication controls risks making his or her business vulnerable to exactly this type of criminal exploitation.

To mitigate the risk of fraudulent credits from entering the payment card system, the following precautions in the sidebar should be taken.

By strengthening authentication credentials and by becoming fully aware of criminal scams and tactics, hospitality industry operators can help avoid criminal exploitation of their payment systems for this scam.

Ingrid Beierly has over 20 years of experience in the information security field. Beierly has been with Visa since 2001 and manages global forensic investigation involving external account data compromises. She has managed some of the world's largest data breaches and has insights on exploits and fraud patterns related to network breaches, malicious software and application vulnerabilities.

Mitigate the risk of fraudulent credits from entering the payment card system.

- Protect merchant credentials and merchant/terminal ID and use strong authentication procedures to access payment gateways and processors. Never use a default password. Criminals are well aware of what the default passwords are, and have been known to exploit this vulnerability almost immediately after new systems are put in place. Likewise, avoid trivial passwords that can be easily broken. Access to authentication credentials should be restricted only to third parties who need access. In many cases, the attack outlined here can be mitigated by the use of two-factor authentication.
- Enable logging on point-of-sale (POS) terminals. Audit logs are valuable in the event of suspected unauthorized activity and for monitoring traffic patterns within your network.
- Protect POS terminals that connect to payment gateways or processors. Do not use POS terminals to browse the Internet or check email.
- Ensure that computer-based POS terminals have the latest anti-virus software and signatures.
- Make certain that employees with access to a gateway or processor system receive proper user training on how to recognize and avoid phishing, voice phishing (vishing) and other social engineering schemes that target merchant credentials.
- Monitor accounts for unusual credits (particularly those with no original offsetting debit, or with the credit going to a different payment card account).
- Report lost or stolen POS terminals to the acquirer or processor and ensure that it blocks all transactions from these terminals.
- Immediately report suspected fraudulent credit schemes to the appropriate law enforcement or regulatory agency and to the acquirer or processor.