My Say (/sites/groupthink/)
Contributor

FOLLOW

Advice and insight from the frontlines of entrepreneurship.
full bio →

Opinions expressed by Forbes Contributors are their own.

(/sites/groupthink/)

Comment Now

Follow Comments

ENTREPRENEURS (/ENTREPRENEURS) 8/06/2015 @ 8:30AM | 495 views

Why Retail Breaches And ATM Hacks Won't Stop -- And How Organizations Can Protect Their Customers

Comment Now Follow Comments

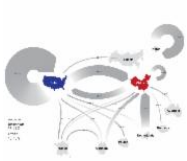
The 2014 deluge of cyber attacks against large merchants like Target (/companies/target/) TGT -0.87% (/companies/target/), Kmart and Home Depot (/companies/home-depot/) HD -0.49% (/companies/home-depot/) was just the tip of a very large iceberg. The success of those breaches is now encouraging hackers to attack even more retailers, some of which are probably already infected. Remember, it took Target *six months* to realize they'd been hacked.

Even worse, a new trend looms that is equally troubling: ATM hacks. The highly publicized Carbanak attack was just the beginning; once cyber hackers realize how old and unsecure the ATM networks are, banks may be in for an unpleasant surprise.

In this article, I would like to discuss the security (http://www.forbes.com/security/) flaws currently impacting the retail (http://www.forbes.com/retail/), banking and payments sectors – and how banks and merchants can strengthen these weak links to prevent breaches, compromised ATMs and stolen customer data.

Problem 1: Outdated Payment Technology

GUEST POST WRITTEN BY
Rod Katzfey
Vice President of Sales Business Development – North America at Credorax



Security Vulnerability Discovered In Millions Of Business Computer Systems - -... (http://www.forbes.com/sites/josephsteinberg/2015/05/13/major-vulnerability-discovered-in-millions-of-business-computer-systems-heres-what-you-need-to-do/)

Joseph Steinberg
Contributor
(http://www.forbes.com/sites/josephsteinberg/)

The payment systems currently in use by most retailers were originally set up in the late 1980s, before the Internet even existed. When e-commerce came along, a concerted effort was made to ensure the security of online credit card payments, but for the brick-and-mortar retailers, the backbone processing platforms never changed.

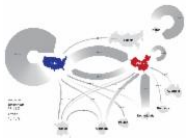
Because retailers are merchants, and not security experts, they generally do not realize that the payment processing technology they are using is very outdated. So not only are they being hacked; they are being hacked without realizing it – sometimes for years.

Banks are experiencing the same issue. How many times in the past few years have you read about major global banking brands being hacked? And most of it is because the payments infrastructure is so obsolete. The same goes for the ATM network. It's been obvious for some time that fraudsters would begin gravitating towards ATMs once they realized how easy it is to hack into the antiquated system.

Problem 2: Lack of EMV Security

In many countries around the world, EMV security has been mandatory for nearly a decade. This has not yet happened in the U.S., and the results speak for themselves: according to the *Nilson Report*, the U.S. accounts for only 25% of global credit card use, yet hosts a full 50% of the world's credit card fraud. There has been a lot of talk about the imminent October 15, 2015 "deadline" for U.S. EMV implementation, but it is by no means the first time a deadline has been set. Every year when the chosen date draws closer, it is evident that retailers will not be ready so the deadline is pushed back.

ATMs would also become much more secure with the implementation of EMV. While traditional ATM cards are only inserted into the terminal long enough for the magnetic stripe to be read (or skimmed by fraudsters), EMV cards remain in the machine for the duration of the transaction, during which unique request and response cryptograms are created, along with other EMV-specific data. Unlike magnetic stripe data, this information is useless to potential hackers and identity thefts.



Hackers Are Targeting Employers Looking To Hire (http://www.forbes.com/sites/josephsteinberg/2015/05/11/hackers-are-targeting-employers-looking-to-hire-here-is-what-you-need-to-know/)

Joseph Steinberg
Contributor
(http://www.forbes.com/sites/josephsteinberg/)

The reason that the U.S. still lacks EMV security is simple: it is going to require a major overhaul of the terminals, which will be both complicated and expensive. You can't have some terminals that are EMV and some that are not; it doesn't work that way. And for years, while fraud levels were low, banks and retailers just wrote off fraud as part of the cost of doing business. But fraud has skyrocketed over the past few years, resulting in loss of not only money but also reputation and public trust. It now makes much more sense for the industry to adopt a more secure solution.

Prevention Tips

It's important to realize that fraud occurs at the point of least resistance. Criminals are trying to do the least amount of work possible; otherwise, they'd have real jobs! And, as discussed, the current Achilles' heel of the financial and retail sectors is the legacy payments systems. Shore up these defenses, and fraud will (at least temporarily) decrease.

The following sections outline specific tactics that retailers and banks can use to prevent fraud and ATM hacks.

Retail Fraud Prevention Tips

- Make sure you put more attention into your payments system, both back end and customer-facing. If you do not have time to do it yourself, hire an outside consultant to look at your system and give advice. A lot of the security bugs can be fixed fairly easily, but they require attention.
- If you're an administrator with control of accounts, change your password once a month. And do not use simple passwords.
- Make sure you are choosing a payment processing provider appropriate for your business. If your emphasis is online vs. offline, ask your provider whether their expertise fits your needs. If necessary, choose one provider for online commerce and a different one for offline.
- Choose the right payment implementation for your business. For example, if you are a small retailer, you can use a Hosted Payment Page, which is hosted on the provider's side. If your provider has a secure system, it's probably safer to do that than to host the payment page yourself.
- Enact policies that weed out fraudsters, including accepting payments only from authorized accounts.
- Pay attention to your customers' IP and mailing addresses: if they don't make sense, do not ship the order.