The Guide to E-Commerce Fraud

Steps to protect you and your customers from digital deceit & theft

Introduction

We're fourteen years into the millennium, thriving in an e-commerce landscape where online merchants offer goods and services to millions of customers worldwide by way of websites, mobile apps, and social media platforms. Unlike decades past, punching credit card digits into a website is no longer cause for caution and fear. Consumers are even comfortable tapping the nine numbers of a social security number into a smartphone. More and more of us are buying, selling, and banking online. Words like hacking, spamming, and spyware don't elicit the historical apprehension that they used to. *MALWARE has been detected,* a computer screen flashes — the alarming pop-up with the yellow triangle and exclamation point. *Okay.* Time to scan for viruses, possibly run an update or two, and return to that Excel document. Get hacked, get spammed, get pilfered, get over it.

But are we taking these warnings too lightly as e-commerce merchants and online retailers? There are those who might argue that we've gotten too complacent with our Internet ways. We sell and buy products on-the-go, verify personal information on upwards eight different devices, and trust emails and software more than we ever have before. Understandably so — endless information lies centimeters from our fingertips. Trust can be a personal preference; however, for the sake of good business, there is an essential need to remain aware of dubious practices, scams, and schemes that exist in the e-commerce domain. We monitor to keep both the company and its customers protected from fraud.

> *"It doesn't operate out of basements or back alleys," the voiceover on the latest American Express commercial informs. "It grows more sophisticated every day. If it were a business, it would be a Fortune 500 Company. Fraud has evolved."*

North American merchants and consumers lost $3.5 billion dollars last year to e-commerce fraud, according to the *Market Overview: E-commerce Fraud*

Management Solutions 2014 Report by Forrester Research. In addition, Businessnewsdaily.com reported that over 20 percent of mobile merchants reported fraudulent incidents last year. On the defensive front, Google just bought Spider.io to crack down on the growing number of ad-click scams. With the upswing of traffic and transactions on the web, e-commerce fraudulence is alive and well in 2014.

Online fraud operates at a very different level then it did a decade ago. This fact is no more apparent than in two very recent examples of e-commerce fraud, which lie on opposite ends of the financial vice spectrum.

The 2013 Target Breach

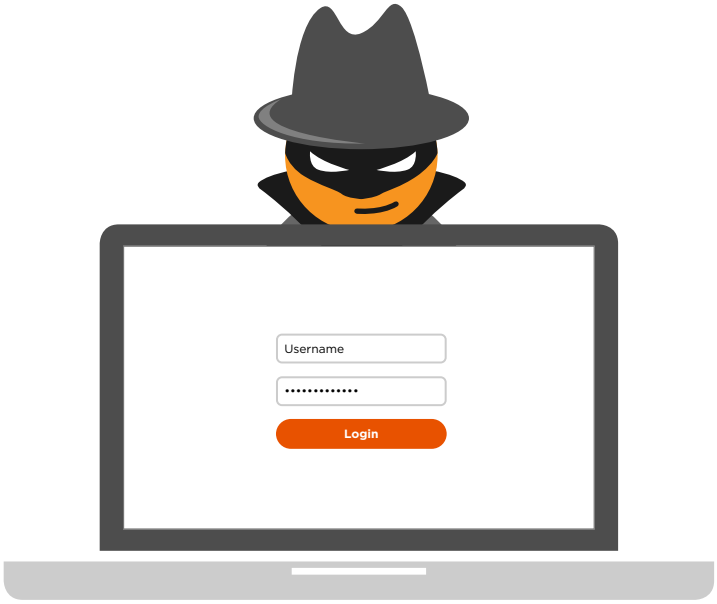
Our first example made headlines in early December when Target admitted that 40 million credit and debit cards were compromised by an unauthorized party. The breach cost the banks (the parties responsible for reissuing those cards) $10 per card, accumulating a $153 million deficit in unexpected expenses. Just weeks after the first breach, Target warned its customers of a second breach; this one jeopardized the names, addresses, emails, and phone numbers of another 70 million. Target was attacked from both sides. The first breach occurred in-store, occurring at a point of sale (POS) device, while the latter went beyond the POS through a backend web portal. In total, one hundred and ten million Target customers either had their personal information (address, email, phone numbers) hacked, their credit and debit card information stolen, or both. Target CEO, Gregg Steinhafel, issued a public apology in the *New York Daily News*, promising zero liability to "Target Guests," assuring customers that the malware has been detected and removed. He also offered free credit monitoring and protection for the following year. His letter was designed to reinforce peace of mind and confirm further protection from all manner of cyber criminal.

The Pony Bot

Believe it or not, it *is* possible to steal intangible, uninsurable cryptocurrency. Last month, a Pony (a cyber-crime ring) botnet (a series of infected computers) stole 85 virtual wallets filled with Bitcoins and other digital currencies, according to the security firm Trustwave. The Bitcoin Foundation (an advocate for the adoption of digital currency) has asked that those who have coins store their currency in an offline location; *The Wall Street Journal* suggested to print off records of the coinage. Trustwave was also the firm responsible for uncovering two million stolen Facebook, Google, Twitter, and Yahoo passwords this past December. The Bitcoin perpetrators are still at large, particularly in Canada where $600,000 in Bitcoins were stolen from Flexcoin's "hot wallet," forcing the Bitcoin bank to close. Bitcoins were believed to be completely transparent and 'unhackable' before this event.

Although the online world has experienced waves of digital security advances in the last year, it's clear from the examples above that companies and e-retailers are susceptible to invasive bad actors — from the inside out in the case of Target — and that the wallet of hard-mined digital dollars can be plundered by a cyber criminal running a web ring. But don't assume that big businesses and Bitcoins are the only victims of fraud: *all* e-commerce merchants are at risk for fraudulent activity. Business owners small and large, corporate or independent, must remain aware of the types of fraud that threaten them, adhere to up-to-date digital security measures, and keep both their customers *and* employees informed. Most importantly, you keep potential buyers at arms length with policies that don't value your consumer's security.

Whether it's one consumer trying to get out of the GoPro purchase he or she can't afford, or underground Internet criminals running a 7-year cyber espionage campaign, combating e-commerce fraud is a 360-approach. In the following pages, 2Checkout will review the dirty dealings on the Internet, from surgical attacks made by crafty individuals to large-scale automated campaigns. We'll address the three main types of e-commerce fraud most common today, explain how companies can identify them, and offer suggestions on how to prevent such occurrences, while protecting your customers' personal and financial information — and ultimately, avoiding financial loss.



fraud type

Account Takeover

Account takeover fraud, the unauthorized access and control of another user's personal information online, is the most prevalent type of fraud in the e-commerce domain. Last year, account takeover fraud (ATO) affected over 13 million buyers. ATO was the e-commerce culprit in the case of Target and Neiman Marcus. ATO, also known as identity theft, occurs when one user obtains the credentials to another user's value storing account. A value storing account can be anything from a bank account to a gaming account to a Facebook profile. According to Javelin Strategy & Research, ATO takes place every three seconds in the United States.

An ATO perpetrator can be anyone from the mastermind behind the Pony ring to a one-time cyber hacker looking for some extra bar cash. In the dark world of cyber crime, ATO is relatively easy to execute, especially for the professional hacker (read: cyber crime ringleaders). Yet, all any one person requires to tap into another user's financial accounts (and their value) is a name and password, which is either acquired by tedious guesswork, purchasing, or deploying more sophisticated malware (more on that later) attacks. Sometimes access can be as simple as answering a security question.

Real-World ATO Scenario: Man-in-the-E-Mail Seattle Scam

Last December, three Seattle businesses were compromised by what is being referred to as a "man-in-the-e-mail" scam. The fraudsters gathered email addresses from each business and then impersonated each company to the others in a series of bogus emails. Each company was under the impression that they were securely sending money to a supplier in China, when in truth, they were filling anonymous criminal bank accounts in the U.S. The FBI reports that the scam amounted to losses upwards $1.65 million.

What is Account Takeover Fraud?

Nearly 40 percent of e-commerce fraud falls under the ATO variety, states Forrester Research. ATO used to be the biggest threat to big banks and lending institutions, but as businesses and websites open up their online channels to satisfy the growing number of customers who want instantaneous access to their products and services with cross-channel convenience (tablets and smartphones included), cyber criminals are shifting their focus. The same tactics that worked on banks (which have since reformed their security measures) work on e-retailers. E-commerce is known as the "low-hanging fruit" in the fraudster world. NuData Security states that any company that has a user account or a membership system is at risk for account takeover fraud.

Once any account information is in the wrong hands, e-commerce companies must beware of the following attacks.

Value Extraction

This type of ATO is most similar to bank fraud. In value extraction, hackers look for an account with a large value or balance, and make one purchase to wipe it clean. This happens most often with debit and credit cards or gaming accounts that contain high-value virtual items. An easy way to flag for this ATO is to monitor spending activity and patterns of customers. If a customer breaks from his or her algorithm or range, there's a decent chance some ATO activity could be involved. **When Buying**: don't use debit cards for online purchases. Why? *Debit cards link directly to your bank account.* Use credit cards instead.

Direct Usage

This is the case of the Facebook friend (same concept applies to Twitter, LinkedIn, Google +, et al.) who perpetually posts links to a rapid weight loss program or a dream vacation. Here, one Facebook user's account invites others to click on an ad, a post, or URL — every click connects a victim to a website or party that scans the visitors computer for sensitive information. As much as direct account usage can occur from an outside party, the same attacks can happen from the inside of a company. The fraudster obtains control of a seller's account where he or she can offer a to-die-for vacation promotion to trusted customers, collect a few thousand — or a million — and cash in elsewhere. Nobody's going on vacation.

Phishing

These email attacks (most of which originate in the United States or Asia) are quickly becoming one of the most common ATOs. Customers receive an email (or a text message: *smishing*) from a trusted company or financial institution that asks for personal information, PINs, and other valued credentials. If successful, the fraudulent party obtains access to the victim's accounts and transfers credit to an outside account. Phishing is more deceptive and insidious than value extraction. This practice relies on the complications that come with building trust, and then redirecting information and transactions. "By compromising the email accounts of buyers and sellers using these marketplaces, fraudsters are able to spoof the emails between buyers and sellers necessary to redirect shipments and payments," says John LaCour, of online security firm Phish Labs.

How to Prevent Account Takeover Fraud

ATO can be a Catch-22 for e-tailers. In order to give the customer more (multiple POS locations and access over multiple devices), companies also open up more doors for cyber criminals to infiltrate the system, to attack trusted members, and to steal personal information from customers. Although the customer comes first, and that relationship is most important, all businesses must also acknowledge that the customer, trustworthy or not, can also be the company's weakest link. Whether by choice, or lack of awareness, customers and users often don't take the proper security measures at their own volition.

A business can require a slew of security questions, use random key generators (CAPTCHA), and only accept strong passwords to help avoid any security liabilties that might occur from the user's end.

Take the following ATO security measures (outside of the aforementioned requirements) to guarantee secure and closely-monitored membership accounts. Learn to verify, monitor patterns, and flag unusual activity. Whether users appreciate it or not, such actions are both for the protection of the company and its customers.

1. ***Use a third-party verification system.*** This is a must to protect credit card transactions. Install a 3D secure system (also known as Verified by Visa or MasterCard SecureCode). This is a third-party verification check that asks the customer to enter a passcode before any purchase.

2. ***Practice Session Linking.*** Large scale ATO can take place within minutes. Session Linking is the concept of tracking all users and all activity that takes place during a log-in session within a short period of time. When multiple users show a similar activity (the same link shared; the same product purchased) in this short window of time, it is cause for concern. Depending on the size of a business, session linking can last anywhere from five minutes to one hour. Generally, cyber criminals have to go to great lengths to get the tools to hack, therefore the chances of an ATO occurring on only one or two accounts is very slim.

   Look for signs of an impending ATO when multiple accounts are:
   - accessed at the same time from the same network, IP address, or device
   - making the same purchase
   - requesting recovery information
   - changing shipping information

3. ***Monitor account behavior.*** A change in both concrete patterns and behavioral patterns can be an indicator of an ATO. *Concrete* patterns include changes in: location, IP address, shipping address, verification information or device. Those '*This email is to notify you that the password for the [Snapchat, PNC, Amazon Prime, Yoga Hive] account for [your user name] has been changed*' really do merchants and buyers a favor. *Behavior patterns* refer to when a user exhibits changes in online engagement and activity — posting, purchasing, duration, hour, and type of engagement. The Twitter user who suddenly blows up everyone's newsfeed with one URL at two o'clock in the morning is not typical behavior for a user who logs in, at most, three times a week.

4. ***Communicate.*** Contacting account holders to ask a few in-flow questions benefits everyone if an ATO is possible. These questions sort out the customers from the criminals through knowledge and response time. Purchase history, previous shipping addresses, and names of friends are all good topics. The more specific the questions, the more difficult it will be for the fraudster to recall correct answers in a timely fashion. Additionally, it is worthwhile to inform employees about the different types and dangers of e-commerce fraud. When people learn not to click on erroneous links, open spammy emails, and readily give out information — be it personal or professional — in great quantity and great detail, the likelihood of suffering a data breach will be reduced.

Phishing Hosts by Country (2013)

1. China

2. United States

3. Germany

4. United Kingdom

5. Canada

6. Russia

7. France

8. Hong Kong

9. Netherlands

10. Brazil

SOURCE: http://www.websense.com

fraud type

Credit Card

A stolen credit card can be acquired in myriad ways. Card Not Present (CNP) credit card fraud constitutes any illegitimate buying and selling transaction that takes place online with stolen credit information: it can involve sales, re-sales, or returns. Before cybercrime flourished, criminals stole credit cards by old-fashioned pickpocketing. Steal the wallet, grab the American Express (company cards are best), and high-tail it down the Jersey Turnpike buying $5,000+ worth of sporting equipment, DVDs, and jeans. Complete the process by ditching the card and re-selling the goods. All the while, the AmEx's legal owner isn't even aware that he or she has a lighter wallet. That was how credit card fraud was executed ten years ago.

The process is far more sophisticated these days. Today, credit card information is swiped via malware (we're getting to that, promise) and various types of ATO. The transactions are considered CNP transactions, and in all cases of Card Not Present, it is the merchant (the seller, the company, the business owner) that loses big. Banks and credit card owners are not liable for the loss.

Real-World Credit Card Scenario: Chicago Taxi Triangulation Scheme

"Use cash for cabs in Chicago," advised First American Bank, which issued a complaint with the City of Chicago a few weeks ago. The bank, which was receiving calls from customers, took notice of "a pattern of fraudulent activity" on debit and credit cards paying for Chicago taxis, alongside American United, Checker, Yellow and Blue Diamond services. "We got calls from several customers, looked at their transactions, and triangulated what was common here," a bank official told Krebs On Security. "We've been complaining to Bank of America, saying 'Hey, do something about this.' They say they couldn't give us any information and that we needed to talk to MasterCard." The details on the fraud and the damage done by this data breach are still to be determined, and it seems as though blame is getting bounced around, which is often the case in these murky triangulation schemes.

What is Credit Card Fraud?

Let's take a look at two widespread types of e-commerce fraud associated with using credit cards. One type involves one person (one user) who makes purchases and immediately demands a refund of the merchant or its credit card provider. The customer will claim that the product/service never arrived or is deficient in some way, and then keep it (after lying that it never arrived or doesn't work). This circumstance defines friendly fraud. In other instances, the customer buys an item from one website and sells it on another. The first website (the merchant) is left dealing with a faulty return: a false chargeback while the fraudster keeps the product and sells it. In either instance, the business loses money and inventory.

Once the credit card is the wrong hands, e-commerce companies can beware of the following attacks:

Friendly Fraud

Also know as the more explanatory "chargeback fraud," "friendly" fraud occurs when a customer makes an online purchase with his or her own credit card and then requests a chargeback (money returned from the transaction for an alleged fault in the product) from the bank or credit card company after receiving the item or service. The chargeback is issued and the financial transaction is canceled. The customer is refunded and, more common than it used to be, the merchant is issued a chargeback fee — upwards of $50 per cancelation.

Ultimately, the consumer keeps the product or service after claiming that he or she never received it or that it was broken or defective. Hence, the consumer receives a product or service for free. When it comes to a chargeback, whether in good faith or not, the merchant is usually responsible (3D-Secure Protocol from credit cards will vouch on the side of merchants in some cases), despite any measures it has undergone to insure a secure transaction and delivery.

There are two types of friendly fraud:

Deliberate: A good-standing customer makes a purchase on a website, then illegitimately disputes the purchase with the credit card company; the merchant is issued a chargeback. This occurs when trusted customers have learned to take advantage of the system, in which instance they are "making" money off of each transaction be lying that the end product wasn't as advertised or never arrived. In other instances, this is the drastic action a customer makes when he or she fears that the purchase will upset his or her financial stability.

Accidental: Similar to deliberate friendly fraud, accidental friendly fraud happens when a customer issues a chargeback as a mistake, and later receives the product or service in dispute. The chargeback goes through, yet the customer does nothing to rectify the situation. In most cases, the seller is able to contact the customer directly and avoid any legal action or financial loss. It is a common mistake when a customer does not recognize the credit card charge on a bank statement or online bill (or the charges of children and family members). This occurs more often in businesses that use a third-party billing service that isn't recognized on a billing statement. An easy way to prevent this particular mishap is to have the billing service or payment service provider's information easily visible on the website of the merchant — especially the billing page — so any information connected to that provider will be readily identifiable.

The Triangulation Scheme

In this credit card scheme, the fraudster purchases an expensive item from *one* e-commerce domain (using a stolen card or employing deliberate friendly fraud) and goes to a *second* website (a seller's website that accepts public merchants, such as eBay) and sells the item to a *third* unsuspecting individual. The faster the transactions occur, the less time either website has to do the appropriate checks and balances to determine the validity of the card, which may be stolen. The fraudulent party is paid by the third party while the original merchant has either accepted payment from a stolen credit card (which will result in a chargeback) or suffers a chargeback as the fraudster claims that he or she never received the merchandise.

How to Prevent Credit Card Fraud

When credit cards are involved, there are less ex-post-facto measures an e-commerce business can take, as credit card fraud falls on the merchant. Fraudsters can prey off merchants and businesses that have a noticeable gap between the seller and the buyer; merchants with this liability will experience this type of fraud the most. This situation allows customers to circumvent the merchant or seller and go straight to a bank or credit card company. Going by the old adage, "the customer is always right," the customer — or fraudster in this case — plays the easy role of the victim, whether he or she was legitimately victimized.

To prevent this type of e-commerce fraudulence, businesses and e-tailers must maintain a tight and trustworthy relationship among the merchant, the buyer and, if need be, the third-party billing or payment provider. Here are a few steps that small and large e-commerce businesses can take to close the gap and discourage fraudsters from stealing merchandise, receiving illegal refunds, and making a dirty profit.

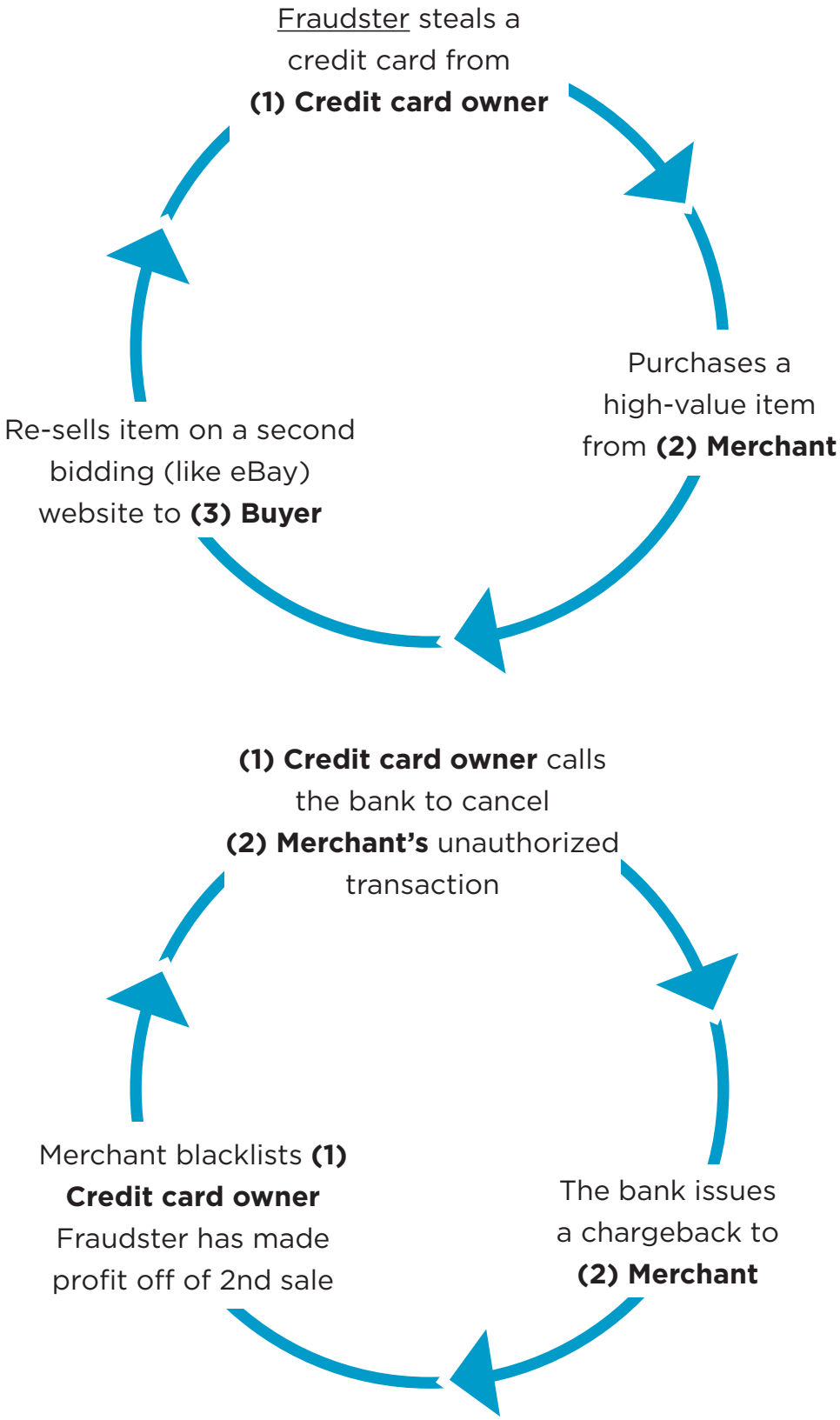
1. ***Keep them close.*** Encourage customers to contact the customer service team if they have any questions at all about shipping, delivery, purchasing, returns, or sales. Give customers and members no reason to contact a financial or lending institution in place of directly contacting the business or the merchant. If the merchant and customer can resolve an issue in-person, a chargeback won't be needed. In turn, make sure that the customer service team is informed, up-to-speed, and exhibits undisputable, excellent service.

2. ***Keep Records.*** Monitor all interactions — phone calls, emails, online chats — between customers and the customer service team. Be ready to reach out when the signs of an impending chargeback appear so that the customer knows that a refund can be properly issued without a financial third party.

3. ***Require delivery receipts on any product that has shipped.*** Have customers sign upon delivery. This action provides more proof, more tangible records that customers have received goods shipped; this information can counteract a chargeback in some instances if a customer signs for a product and later disputes that he or she never received it.

4. ***Use a "soft descriptor."*** This type of copy is used to keep suppliers and credit card companies aware of the product purchased and to keep consumers accountable for what they've purchased. A soft descriptor looks something like this: *mybusiness 444-123-5678 NM $57.00*, and will appear on bills and statements. This soft descriptor ensures transparency between the customer and merchant as it outlines exactly what and how much a product costs.

The Cycle of Triangulation Fraud: 3 Victims



fraud type

Malware

There are 111,111 unique strains of malware deployed each day, estimates Aite Group. With malware, we're discussing that incredibly annoying desktop pop-up we've all seen: '*Malware Detected! Danger: Malware Ahead!*' that blinks repeatedly until you either choose to close the alert or run the suggested virus scan. Malware is malicious software that collects data or controls computer resources without the knowledge and consent of the user. It's not so much its own form of fraud, as a technology that helps elevate and enable it to a whole new level of harm. Just ask Target, as malware was the cyber criminal tactic used for their second security breach last December.

Real-World Malware Scenario: Careto

Careto is Spanish for "The Mask": it's a 3-tiered (Mac OS X, Linux, and Windows) backdoor malware program that targated an estimated 1,000 IP addresses throughout 31 countries in 2012 by way of URLs impersonating a slew of Spanish newspapers, along with such ubiquitous publications as "The Guardian," "The Washington Post," and "The Independent." The hackers behind Careto successfully aimed and captured large lists of documents from the infected systems, including encryption keys, VPN configurations, SSH keys, and RDP (remote desktop protocol) files. The computers attacked belonged to government institutions; embassies and other diplomatic missions: energy, oil, and gas companies; research institutions; and private equity firms and activists. "There are also several extensions being monitored that we have not been able to identify and could be related to custom military/government-level encryption tools," said the team of anti-virus researchers at Kasperky Labs. The Mask: Cyber-espionage at it's finest.

Currently, little is known about the effects of this breach. The attackers have recently backed down and stayed offline, but it's been said that Careto has been running rampant since 2007.

What is Malware?

Malware puts both companies and their customers at risk for credit card fraud and account takeover fraud. Many traditional fraud prevention tools analyze the user's device to verify the user against previous or public information, assuming that the person operating the trusted device is the trusted user, and is therefore safe. Malware breaks this model. There are several red flags to identify a device plagued by malware. If a device is connecting from Africa, for example, when the customer resides in Maryland, then that's a red flag. If a device shows a change in IP address? Red flag. If a device shows an excessive amount of unusual outbound traffic (emails, posting, file transfers): also a red flag.

Malware's goal is to deceive. When a user's computer is infected with malware, both the legitimate user and the legitimate device are involved in the transaction. The customer enters into a transaction with your business in good faith. They are generally unaware that their device harbors malware.

Once the user's device is infected by malware, e-commerce companies can beware of the following attacks:

Spyware

Also known as a *keylogger*, this software infects devices (computer, smartphone, or tablet) by latching onto a user's login and eavesdropping on the user's session activities. Spyware often looks for patterns in keystrokes that lead to account numbers, credit cards, verifications, and other valuable and personal information. In the crime underworld, spyware software costs as little as $50.

Backdoor

Affectionately nicknamed Trojans, this malware operates just like the Trojan horse of Greek myth, sneakily infiltrating a healthy computer with a hidden bad program. The easiest and most common instance is called a "drive-by-download." A user clicks on a link from his or her computer, smartphone, or tablet and chooses to either: upload, install, or download from a compromised URL. Backdoor malware is a notch up from spyware in terms of complexity and harm. This breed of malware is about spying or eavesdropping to gain info, but it also disperses strands of malicious code (enemy soldiers, for those of us sticking with the Trojan analogy). Backdoor malware aims to keep the infection going, spreading the bad code from machine to machine.

C&C

This abbreviation stands for Command & Control. It's the worst form of malware. Cyber criminals who have purchased cheap spyware will often invest in a botnet (like Pony): a ring of computers to infiltrate private information. Botnets can cost as little as $18. These bots are responsible for continually sending spammy emails or suspicious ads with compromising code out to bigger networks. C&C delivers malware like a tweet gone viral. Tweet to five followers, who tweet to five more; 25 tweets morph into thousands, maybe millions. Who was it that tweeted what again? Which computer? The question of which computer spreads C&C is rarely answered, because bots don't attribute information. Thousands of computers are affected with every click-through opening a door to infect a new healthy computer.

Here are a few other strains of malware to look for:

- **Scareware**: a fake virus (the only time when you should *not* download the anti-virus protocol)
- **Adware**: banner ad software or pop-ups that replace legitimate, online advertisements
- **Email Spam**: fake emails that contain fraudulent URLs

How to Prevent Malware

Before addressing technical precautionary steps to prevent malware infections, please ensure personal and professional machines are protected with these three simple checks (this goes equally for Macs and PCs). (1) Install the latest security software from your system's designers; the same goes for Androids, iPhones, and other smartphones. (2) Install and update third-party anti-virus programs. PCMag.com features a round up for Macs, as well as one for PCs. (3) Set the program to update to the latest malware definitions. Make sure the program regularly performs all-system scans, which a good program will. Do any less than these three, and you leave your company open to a security breach.

Now, on to even more precautionary measures to keep all systems and devices free of cyber infection and infiltration.

1. ***Keep it separate.*** There are two methods to keep your digital assets segregated so malware can't infect your entire system: do both. (1) Create one separate administrator account *only* to be used when installing, updating, and deleting software. Do not search, browse, or hop online with this account. Don't even read emails. If this account is infected, you can delete it without touching the rest of your work partitioned elsewhere on your computer. (2) Do not grant users (customers) any type of administrative access, or allow them to make changes to the operating system.

2. ***Use Firewall Security.*** This is a barrier between a trusted, internal, and secure network (your business), and any other network (the Internet). A firewall won't allow certain types of information through. With a firewall, a company can set up specifications, *I.E. only one computer out of many is able to receive traffic from an FTP server.* Keep an additional firewall between the application server and the database server, which will significantly minimize the risk of malware infection from an online web server, advises Derek Hitch, of the blog Tweak Your Biz.

3. ***Use strong passwords.*** Yes, this also goes for members, users, and customers, but as previously noted, the customer is king (or queen), and nothing can be forced upon him or her. However, internally, all machines and employees need to have very, very strong passwords that should be changed quarterly.

   Here are general shoulds and should nots for creating passwords:
   - Passwords should not contain a complete word
   - Passwords should be at least eight characters long
   - Passwords should not contain: your name, your username, your company's name
   - Passwords should be significantly different than previous passwords
   - Passwords should contain all four: an upper case letter, a lower case letter, a symbol and a number

4. ***Don't forget mobile devices*** Apple users: avoid any "jailbreaking" tactics and install regular IOS updates. Droid users: Install Mobile Security Software. And *never* install a system update that pops up on your screen. You can always check Android Official Blog to see what is new and upcoming.

A Worldwide Leader in Fraud Prevention

2Checkout wields an array of state-of-the-art tools that stops fraud before it starts.

- Our fraud network employs a patent-pending technology that connects consumers, merchants, issuing banks, and credit card associations in an online network of trusted relationships
- We currently detect 600 million devices using a unique, patented tagless device identification technology
- We use patented link analysis tools to correlate seemingly-unrelated events that other solutions might miss.

These technologies eliminate the anonymity of the Internet, protecting sellers from fraud from every angle possible.

Premier Technology and a Zero Tolerance Promise

Our fraud prevention technology uses a rules-based risk engine that works on a fire-and-continue methodology to prevent fraud. We allow good transactions to process as quickly as possible while screening unwanted intrusions.

Our technology analyzes every transaction to determine its level of risk, combing through data for signs of intentional deception. Once a transaction is flagged as suspicious, our technology alerts our internal fraud team to rapidly assess the transaction.

Sell Securely

2Checkout's fraud network uses a patented tagless device ID technology removes anonymity for 600 million devices. Fraud thrives on the World Wide Web because of the anonymity it can provide to scammers and fraudulent parties. Our fraud technologies are designed to create a transparent and controlled environment, effectively holding each buyer responsible for his or her actions. Our tagless device ID analyzes myriad variables on each device, ascribing a unique fingerprint to each variant of device. If we see nefarious activity from the same fingerprint, it's automatically flagged and detained.

Have questions about these principles and tips or want to share your experience with applying them?
Connect with us on Twitter, Facebook, or LinkedIn.

share

Accept Payments, **Globally**

A worldwide leader in payment services, 2Checkout maximizes online sales conversions by giving global buyers localized payment options. Trusted by over 50,000 merchants, 2Checkout supports transactions in 196 countries through 8 payment methods, 26 currencies, and 15 languages, forming one of the leading processors of online transactions in the world. The service is simple to implement, including a pre-integrated payment gateway, a merchant account, PCI compliance, international fraud prevention, and plug-ins for 100 of the most popular carts.

Connect with 2Checkout and learn more about how our services can empower you to sell safely and securely.

Connect >>

about the author

Janna Leyde

Janna is a writer and published author living in Pittsburgh, PA. She holds her master's in journalism from New York University and is a regular contributor to various magazines, blogs, and websites on topics ranging from healthy living to effective marketing. When she's not working with words or marketing campaigns, she teaches yoga.