eBook

Top 10 Anti-fraud Tips: The Cybersecurity Breach Aftermath

Protecting against downstream fraud attacks in the wake of large-scale security breaches.

ThreatMetrix®

Digital companies can no longer trust static login and user credentials.

In the wake of numerous large-scale data breaches, stolen data such as login credentials and payment details is being widely leveraged by cybercriminals for fraudulent activity, for example on online banking and e-commerce sites.

To compound the problem, cybercriminals are able to dramatically increase the efficiency and scale of such attacks by using bots and botnets to run massive identity testing sessions in order to penetrate fraud defenses. The recent trend towards low-and-slow Bot attacks can often bypass traditional security defenses such as Web Application Firewalls.

How do organizations continue to successfully operate online in this world of digital debris? Here is guidance on how to accurately authenticate your users in real time, and secure against fraud and account takeover attacks.

Top 10 Anti-fraud Tips: The Cybersecurity Breach Aftermath:

Tip #1

Device identification is the first perimeter of defense to protect online transactions.

Every interaction a consumer makes with a website leaves a digital footprint about the device, browser and connection used. This can be leveraged to match users' desktop and mobile devices to their login credentials, giving a layer of authentication that is totally invisible to the user and thus avoids adding friction. Ensure that you identify devices not just by cookies, which can easily be wiped, but with full profiling of device characteristics such as browser, operating system, language and time zone settings.

Protect against downstream fraud by assessing:

- Device history: is this device linked with transactions and account activity from this user?
- Device reputation: has this device ever been involved with fraud?
- Anomaly detection: are there any suspicious computer configurations?

Tip #2

Use **behavioral profiling and analytics** to monitor for suspicious patterns of login requests or transactions, based on account history and persona identifiers.

Digital transactions continue to proliferate as consumers buy goods and access services and content online. As they go about their lives online, each user leaves a digital footprint that can be used to understand whether a transaction is legitimate or fraudulent:

- **Behavior variables**: Over a period of time, track how quickly or often transactions normally occur to create an expected pattern of behavior. Use this to quickly distinguish a returning customer from a cybercriminal displaying known fraudulent behaviors.
- **Age variables**: Measures such as the time since the first event, time since the last event and average time between events can create a profile of a consumer's activity patterns and enable you to spot fraudulent or scripting attacks.
- **Location and distance**: Customers' location and travel behaviors provide valuable insights that establish normal usage vs fraud. Analyze your consumers' trusted location, distance from the trusted location and also the distance between events.

Tip #3

Ensure you are equipped to detect **evidence of malware** on a legitimate user's login session.

This includes keyloggers, Trojans, Man-in-the-Browser and Man-in-the-Middle attacks.

Cybercriminals have a wide range of malware at their disposal, which is used to collect critical personal or payment information as well as to fully control any Web sessions from an end user's device. In the wake of major security breaches, individuals are especially vulnerable to phishing attacks that infect users with malware. The Zeus Trojan is one of the most prolific and high profile MitB Trojans and despite its well-understood technology is still the most successful Trojan today. Trojans are designed to modify any website according to their configuration so that users cannot distinguish which parts of the website are legitimate and which parts are injected using the MitB Trojan. Often the user is unaware they have been compromised.

- Detect malware present on devices through malware forensics
- Understand attack patterns and identify contextual patterns which relate to malware attacks
- Employ malware detection techniques that work in the background without relying on user downloads or registrations

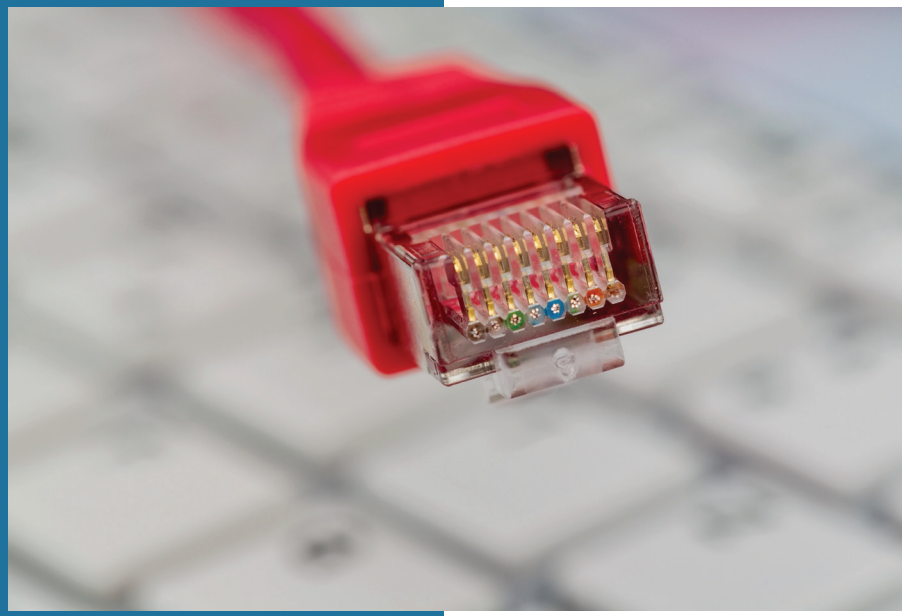
Tip #4

Prepare for **non-signature-based malware detection**.

Although anti-virus software is helpful in reducing machine resident malware, it often gives a user a false sense of security against malware. Even when anti-virus is kept up to date, it cannot protect against zero-day attacks.

Employ techniques such as advanced page fingerprinting, which detects Web page elements that have been altered, rather than relying on signature-based malware detection.

Criminals are taking advantage of high-profile security breaches to get in touch with individuals and trick them into installing Remote Access Trojans. Banks are being actively targeted by fraudulent transactions made by criminals using these RATs. These are difficult for regular anti-fraud techniques to spot because the users' credentials, location and device will all appear completely normal. This is where behavioral analysis is vital to detect this anomalous activity. These attacks often target high-value transactions and can have disastrous consequences for the victim if they fail to be thwarted in real time.



Tip #5

Monitor for **risky devices and IP addresses** which have been involved in attacking other websites, or which are **accessing multiple accounts** from the same device. Leverage **global threat information**, including known fraudsters and botnet participation, to block their attacks.

In the wake of major security breaches, cybercriminals employ bot and botnets to carry out large-scale testing of stolen data - in order to then go on and use this data fraudulently. Due to a shift toward “low-and-slow” bot attacks, they are increasingly able to stay below the detection threshold of existing Web security defenses. However, these major testing sessions leave an unmistakable global footprint when assessing transactions from multiple websites. It is only by accessing intelligence from outside your own perimeter that you are able to get true insight into whether you are being targeted in these attacks.

Tip #6

Look out for **suspicious computer configurations**.

This includes oddly-configured mobile devices, devices which are disguising their true geo-location with hidden proxies or which are on the Thor network. Cybercriminals use increasingly sophisticated methods to hide their true location and IP addresses. On the other hand, legitimate users will not go to such lengths to cover up their location, so any attempts to do so should be a major red flag when monitoring for fraud. Employ proxy-piercing technologies to expose the true IP address of a cybercriminal in order to unmask fraudulent activity. Look out for spoofed devices and device manipulation, both of which could indicate malicious intent.

Tip #7

Reduce reliance on step-up and **“out-of-band” authentication.**

Employ these techniques for suspicious and high-risk logins only. Even in the context of the high-risk cyber threat landscape, minimizing friction is still a top priority when it comes to authentication.

Due to the number of data breaches we have seen and the high stakes involved for businesses that are affected, security teams have put many steps in place to protect themselves and their online users from fraudulent activity. However, this can be at odds with the commercial targets of the business.

In today’s fast-paced digital world, providing an exceptional customer experience is critical for keeping customers and driving revenue online. A traditional anti-fraud approach that makes your consumers jump through hoops just to prove who they are is no longer viable. As consumers are logging into numerous sites in their daily personal and professional lives, services that are hard to access will end up losing out to competitors.

Employ a risk scoring approach when analyzing transactions in real time, using step-up authentication as a last resort when the risk is deemed to be elevated.

- Provide a frictionless online experience
- Drive up conversion rates and online revenues
- Decrease the operational costs of employing costly two-factor authentication methods

Tip #8

No man is an island: **Leverage global shared intelligence** to authenticate your users based on their true digital identity.

Each time a network is breached, every online business becomes vulnerable to the digital debris. Following high-profile data breaches, pieces of a user's digital identity – including email addresses, phone numbers, Social Security numbers and more – can be used repeatedly by fraudsters.

To proactively thwart cybercriminals, businesses need to look beyond their own firewalls to share actionable threat intelligence about compromised identities and devices. Gain insight into your users' true digital identities by leveraging global shared intelligence taken from the analysis of transactions across many websites and industries to detect when personal information and devices are being used illegitimately based on historical norms.

Tip #9

Avoid lots of technologies working in silos to authenticate users; instead, get a **holistic view of users' identities** to protect against fraud.

A traditional cybersecurity approach using multiple technologies from different vendors is costly, complex and inefficient; requiring integration across technologies and data silos. It is difficult to get a common view of devices and users across all systems. Cybercriminals can slip through the gaps, particularly with attacks using multiple vectors.

Employ a holistic approach that integrates malware detection, identity analytics, device identification and behavioral analytics into a single unified view of the risk associated with that event. Protect the integrity of online transactions and identities with increased accuracy, efficiency and in a more cost-effective manner.

Tip #10

Ensure you have mechanisms in place to **instantly recognize returning customers** with no evidence of malware, tampered login details or compromised devices.

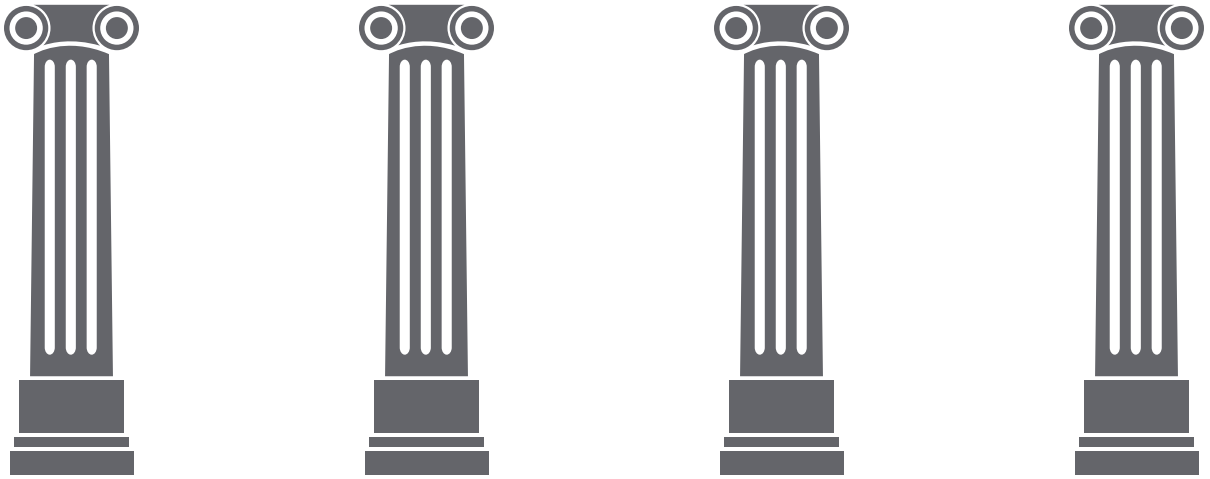
Every day, online businesses turn away commerce from loyal customers because their fraud systems lack the intelligence to identify that they are genuine, and because customers are turned off by burdensome authentication processes.

The traditional approach puts the burden of authentication on customers, often involving changing forgotten passwords or other verification details, making the process complex, time-consuming and too much effort.

Remember, 95% of online activity is genuine, so ensure that you focus your efforts on the instant recognition of returning customers. Employ an intelligent customer authentication approach that is based on an established digital footprint in order to ensure a first-class customer experience for trusted users.

The Four Pillars of Digital Identity

The ThreatMetrix Digital Identity Network addresses downstream fraud due to compromised login credentials and personal & financial data. It combines the 4 key pillars of Digital Identity to facilitate real-time authentication of genuine users and transactions versus fraudulent activity:



Device Profiling

Persistent and statistical web and mobile device identification, profiling operating system, browser, internet connection and more.

Threat Intelligence

Harnessing point-in-time detection of malware, RATs, automated bot attacks, session hijacking and phished accounts and combining with global threat information including known fraudsters and botnet participation.

Identity Data

Analysis of anonymized, non-regulated personal information such as user name, email address, telephone, address provided at the time of a transaction.

Behavior Analytics

Defining a pattern of trusted user behavior by combining identity and transactional metadata with device identifiers, connection and location characteristics.

About ThreatMetrix

ThreatMetrix®, The Digital Identity Company, is the market-leading cloud solution for authenticating digital personas and transactions on the Internet. Verifying billions of annual transactions supporting tens of thousands of websites and thousands of customers globally through the ThreatMetrix® Digital Identity Network, ThreatMetrix secures businesses and end users against account takeover, payment fraud and fraudulent account registrations resulting from malware and data breaches. Key benefits include an improved customer experience, reduced friction, revenue gain, and lower fraud and operational costs. The ThreatMetrix solution is deployed across a variety of industries, including financial services, e-commerce, payments and lending, media, government, and insurance.