PYMNTS.com

DIGITAL FRAUD TRACKER®

How DocuSign Keeps Phishers From Hooking Its Data

FEATURE STORY
Page 6

JANUARY 2020

DATAVISOR

DIGITAL FRAUD TRACKER®

ACKNOWLEDGMENT

The Digital Fraud Tracker® was done in collaboration with DataVisor, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

PYMNTS.com | DATAVISOR

WHAT'S INSIDE

The first half of 2019 saw more than 4.1 billion consumer accounts compromised in data breaches, costing businesses nearly $4 million per incident. One hack occurs approximately once every 39 seconds, according to recent research, affecting companies and consumers worldwide.

Phishing is one of the most pernicious digital fraud forms and sees fraudsters tricking victims into giving up login credentials or other sensitive information, which is sold on dark web marketplaces or used to hijack accounts. Such attempts increased roughly 65 percent in 2019 and were responsible for more than $12 billion in business losses. They also affect individuals, with Verizon reporting that targeted users read 30 percent of all phishing messages and that 15 percent of victims were targeted again within a year.

The cybersecurity space is growing just as quickly to combat this wave of attacks. It is currently valued at approximately $120 billion and is expected to reach more than $300 billion by 2024. A recent report projects the industry will be responsible for more than 3.5 million jobs by 2021, up from just 1 million in 2014. The cyber insurance market will likely also see growth, with research noting that it is currently responsible for $2.4 billion in premiums — an amount that is predicted to double or triple by the end of this year.

Cybercrime-related losses may be increasing, but the efforts devoted to stopping them are also on the rise. These initiatives will need to be both comprehensive enough to stop fraudsters and seamless enough to avoid hampering the growing digital economy.

DIGITAL FRAUD DEVELOPMENTS AROUND THE WORLD

One such effort comes from India's Ministry of Consumer Affairs, which is considering regulations to prevent fraud on social networks like Facebook, Instagram, Pinterest and WhatsApp by bringing them under the same rules followed by other eCommerce businesses. There has recently been an increase in fraud on these social marketplaces in the country, with 46 percent of residents reporting being scammed on such platforms.

Fraud statistics are even more jaw dropping in the United States. A recent study found that 90 percent of Americans have falle victim to online scams, data breaches, identity theft or other fraud forms. The most common attacks were online scams, with fake money transfer requests affecting 63 percent of respondents, for example. Many of those surveyed admitted to partaking in risky online behaviors — like responding to unsolicited romantic requests — that increase the chances of being defrauded.

Fraud targets municipalities as well as individuals, with New Orleans being the most recent victim of a city-scale cyberattack. It declared a state of emergency after being hit with ransomware in December 2019

that infected more than 4,000 government computers. The city shut down its entire network to prevent the virus's spread, rendering many services unusable and causing more than $1 million in losses. New Orleans experienced a similar attack earlier in 2019 that forced its Office of Motor Vehicles to close for several days. More than 40 other cities have reported such breaches.

For more on these stories and other digital fraud developments, read the Tracker's News and Trends section (p. 10).

HOW DOCUSIGN ICES OUT PHISHING ATTACKS

Phishing scams are some of businesses' worst fears, as a single employee's slip-up can potentially cost firms not just millions of dollars but also customers' trust. These attacks are an especially pertinent concernfor DocuSign, which processes hundreds of millions of electronic signatures annually, making it a prime phishing target. In this month's Feature Story (p. 6), PYMNTS spoke with Emily Heath, DocuSign's chief trust and security officer, about how the company leverages both threat intelligence and employee awareness to protect itself and its users.

DEEP DIVE: BUSINESSES STRUGGLE WITH EMPLOYEE PHISHING

Data breaches cost firms significant amounts of money, with recent research finding that the average price tag of a single breach rose 1.5 percent in 2019 to $3.92 million. Many businesses are shoring up their infrastructures and security efforts to thwart cyberattacks, but their employees could be their greatest vulnerabilities. Cybercriminals employ a number of techniques — especially phishing — to attack and exploit companies' in-house and remote workers. This month's Deep Dive (p. 14) explores the threat phishing poses, as well as the steps companies can take to prevent bad actors from taking advantage of employees.

EXECUTIVE INSIGHT

Looking into 2020, what are some of the emerging fraud types that merchants must watch out for?

"As we enter the new decade, the battle between businesses and fraudsters … is scaling to new and ever-more dangerous heights. Digital threat attacks today are highly sophisticated — they come fast, at massive scale and the potential for damage is almost immeasurable. … For merchants, the ability to act early, proactively and in real time is not a luxury. It's mandatory if organizations expect to successfully protect their businesses, their data and their customers.

Fraudsters can rely on a steady stream of sensitive information leaked in data breaches to fuel their criminal efforts, and bots enable them to massively scale their attacks. … To simultaneously prevent … attacks and preserve customer experience, real-time detection capabilities are essential. … Fraudsters [are becoming] more adept at obfuscating their efforts, and [it is becoming] increasingly difficult to distinguish legitimate user accounts from fake and malicious ones, [putting] merchants … under overwhelming pressure to make … assessments without introducing new frictions.

… Phishing, credential stuffing and social engineering have become … widespread, identity theft is rampant and damage from content abuse, buyer-seller collusion and application fraud continues to worsen. [These] problems are compounded by speed, scale and, increasingly, duration. Sophisticated digital … attacks can last anywhere from one day to [several] weeks and can literally double in size overnight. Fake accounts can be used in attacks almost immediately upon registration, or incubated for weeks.

… Transformational technologies such as unsupervised machine learning enable the real-time responsiveness necessary to stop fraud at the gate. In 2020, the sophistication of modern digital threat attacks should be of grave concern to all merchants across all organizations doing business in the digital economy, and their focus should be on integrating and deploying the … tools necessary to defeat even the most [advanced] attacks."

YINGLIAN XIE

co-founder and CEO at DataVisor

5 FIVE FAST FACTS

90%

Portion of data breaches caused by phishing in 2019

15%

Share of low-sophistication attacks that last for just one day

$1M

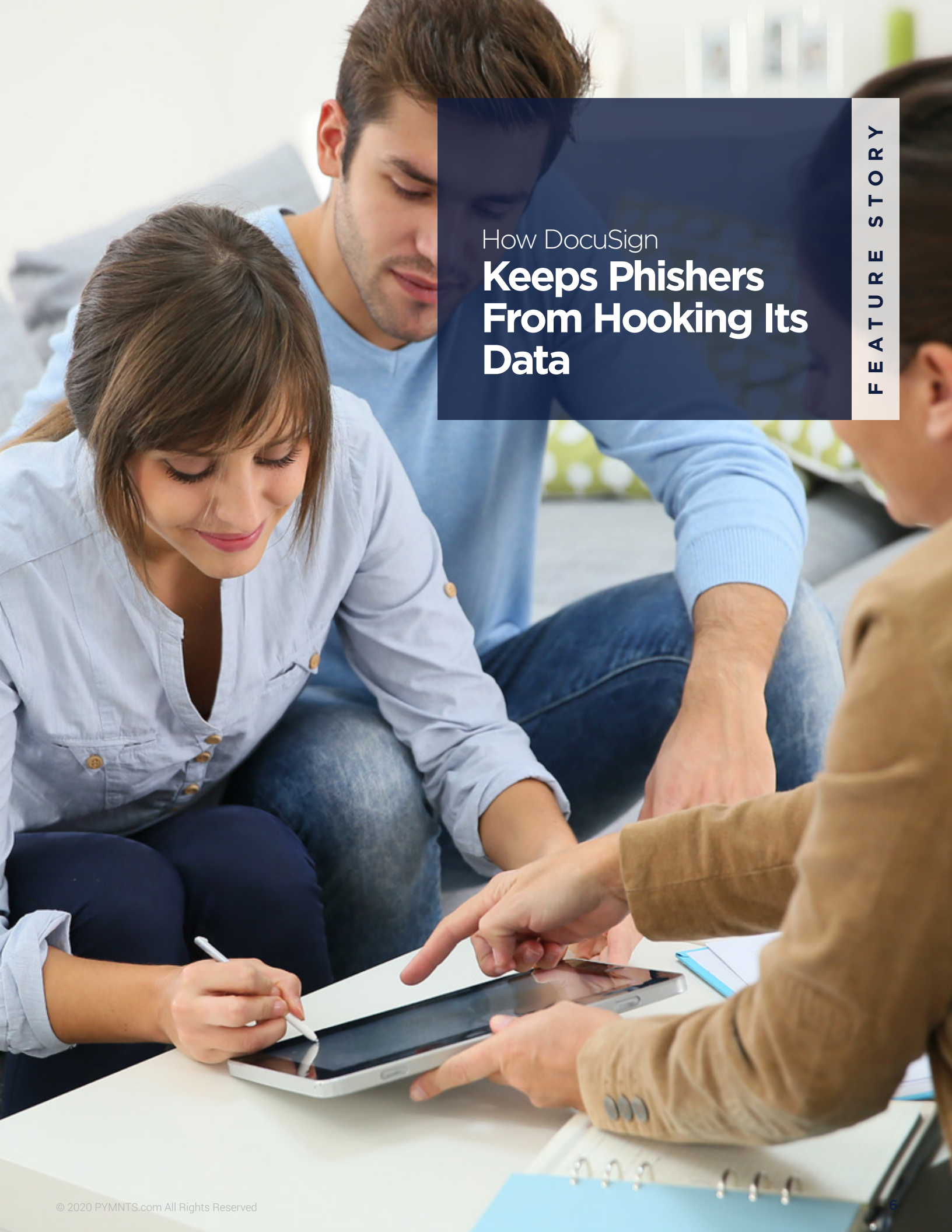
Current losses from a cyberattack that targeted New Orleans

20%

Share of ad requests that were fraudulent in 2019

5%

Decline in Australia's fraud losses for the 2018-19 financial year



FEATURE STORY

How DocuSign

Keeps Phishers From Hooking Its Data

FEATURESTORY

Successful phishing attacks are among many businesses' worst fears. Fraudsters who gain access to employees' login details can cause untold amounts of damage, including emptying corporate bank accounts and exposing terabytes of customers' personal information on the internet. Compounding this fear is the ease with which fraudsters can conduct these attacks. Sending out thousands of attempts every minute is simple and requires only one employee to unwittingly play into hackers' hands for fraud to take place.

"Phishing is always the number one cause of [security] incidents, not only for DocuSign, but also for every other company I've ever worked for," Emily Heath, chief trust and security officer at electronic signature provider DocuSign, noted in a recent interview with PYMNTS.

DocuSign has more than 500,000 paying customers and processes hundreds of millions of electronic signatures annually, making it a prime target for phishers looking to exploit personal information. The company leverages both threat intelligence and employee awareness to keep it, its workers and its customers safe and believes that understanding fraud is a major component to combatting it.

TRACKING PHISHERS' ANGLES

Phishers targeting DocuSign are typically after users' credentials, such as identifying information, passwords and usernames, according to Heath. These details can be used to either log into employees' DocuSign accounts or launch hacks on other websites.

"Human nature tells you that normally people use very similar or the same passwords [on] multiple [sites], so [the fraudsters] will try credential stuffing [on] a number of different sites, including bank [websites]," she said.

Phishing attacks often take one of two forms, Heath explained. The first consists of links to fraudulent websites, inviting users to enter their usernames, passwords or other credentials. These sites' interfaces are nearly indistinguishable from the legitimate login screens to which users are accustomed, but they lead nowhere and send entered credentials directly to the schemes' perpetrators.

Another prevalent type of phishing email tricks users into downloading attachments that install malware on their computers. This tactic accomplishes the same objective as the fraudulent link — stealing login credentials — but grants even broader access to victims' systems, enabling bad actors to pilfer all saved passwords, rather than just the one entered.

Protecting against these attacks is a top priority for DocuSign as just one slip-up could spell disaster for the victimized staffer as well as the entire company.

KNOWING IS HALF THE BATTLE

DocuSign guards its staff against phishing with a two-pronged approach, the first part of which involves a thorough understanding of the potential threats. The company has a dedicated team of security professionals that scours the dark web for phishing attacks and other potential security issues, allowing DocuSign to proactively determine problems and formulate strategies.

"We have both open source and subscription-based threat intelligence feeds that give us information on the types of phishing activities and malware campaigns that may be out there," Heath said.

Threat intelligence is especially important in determining the source of the threat, as phishing attacks can vary in execution and data based on who is conducting the schemes. The challenge lies in identifying the exact culprit in a sea of look-alikes.

"You could have two phishing emails side by side, but they look exactly the same," she said. "One of them could be sent from the Chinese nation-state and the other one could have been sent from Joe Criminal sitting in a Starbucks. Although they look the same, the intents and the consequences of those attacks are very different."

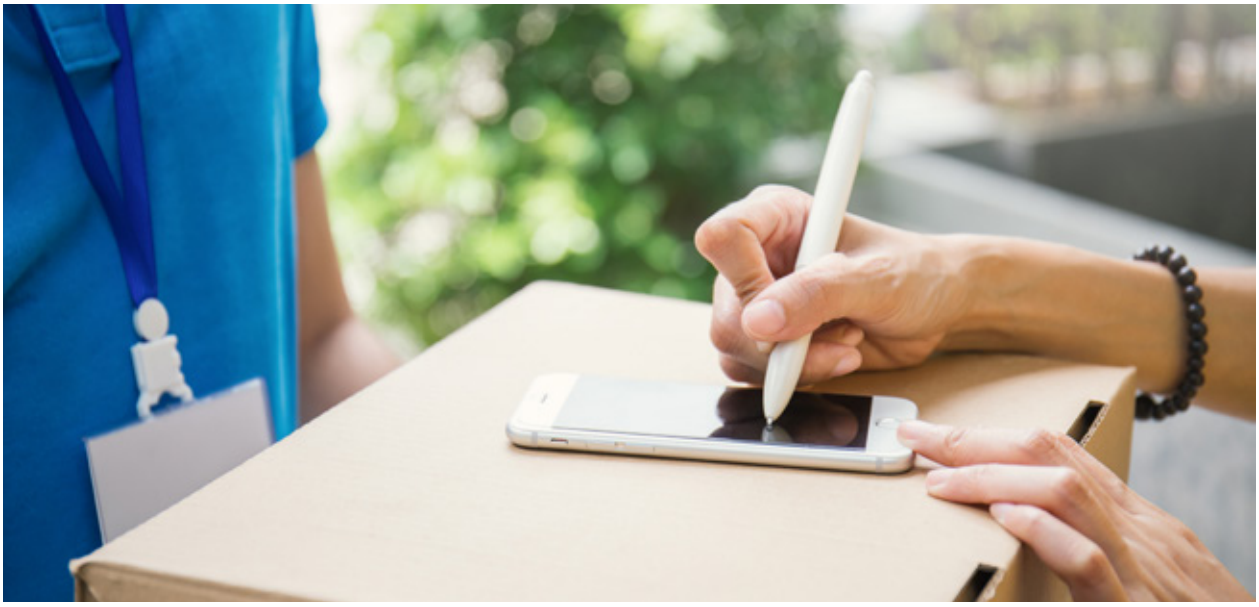
Determining the attribution of the phishing attack helps DocuSign not only figure out how to stop it, but also make informed predictions about how the phisher will attack next.

SMARTER EMPLOYEES ARE SAFER EMPLOYEES

Threat intelligence is only half the equation, however. Employee education is the other key component to DocuSign's anti-phishing efforts, but this does not just involve best practices and classroom instruction. The company also conducts simulated, quarterly campaigns that test employees' abilities to identify phishing emails and bring them to security experts' attention.

"Sometimes employees get a little upset that we're doing simulated phishing exercises, but if anybody's talking about security, that's a really good thing," Heath said.

These campaigns test employees' awareness of phishing and provide DocuSign's security staff with valuable insights and data. The team monitors the click rates of these phishing drills, which grants insights into the



efficacy of its education efforts on an office and departmental level.

"If we see, for example, that the Tel Aviv office has an increase in that click rate, then perhaps it tells us we need to focus some additional education and awareness campaigns for that team," she explained. "But, if we see the human resources team has gotten a lot better, then perhaps we might want to reward that."

Employee education has grown difficult as phishers become more sophisticated in their techniques, though. The best practices of the past do not always cut it in the modern phishing environment.

"A few years ago, the attackers would commonly have spelling mistakes and we would educate people about that," Heath said. "But now they're getting a lot slyer, and it's almost as if they've integrated design into it themselves because a lot of these emails are just so well-written. So, the education has to go a step further as to inspire curiosity."

Recipients should consider whether they actually expected an email from the sender, for example, or look up the email address if they do not recognize it. DocuSign even encourages employees to call the sender on the phone if something is out of the ordinary, arguing that it is better to take up a few moments of someone's time with a false alarm than unwittingly compromise the company's entire network.

Businesses should keep themselves up to date on the best security practices for countering phishing attacks. The consequences of negligence, as seen in a host of recent data breaches, are nothing short of catastrophic.

NEWS&TRENDS

RECENT ATTACKS

TRAVELEX SHUTTERS ONLINE SERVICES FOLLOWING CYBERATTACK

January has seen a variety of cyberattacks, with London-based foreign currency exchange corporation Travelex being one of the most recent victims. The firm was the target of a software virus on New Year's Eve that pushed it to take all services offline to guard against further breaches. A Travelex spokesperson said no personal data or payment information was compromised, but the shutdown forced the company to use entirely manual currency exchange services at its branches. The move cut off a major revenue stream and highlights the secondary effects of cyberattacks. The virus did no direct damage, but the costs of Travelex's safety measure will likely be massive.

NEW ORLEANS DECLARES STATE OF EMERGENCY AFTER RANSOMWARE ATTACK

Cyberattacks commonly target corporations, but municipalities can also fall victim. New Orleans shut down all city-owned computers and declared a state of emergency after being hit with a ransomware attack in December. More than 4,000 computers were infected after a city employee supplied a hacker with login credentials through a phishing scam. The city's computers have since been unusable, and it has suffered more than $1 million in losses. Its online payment systems, such as those for property taxes, are currently inoperable, and it is unclear whether the computers will be back online by Jan. 31 — the property tax due date.

New Orleans was hit earlier in 2019 with an attack that forced its Office of Motor Vehicles to close for several days. Mayor LaToya Cantrell announced plans to increase the city's 2020 cybersecurity insurance policy to $10 million in light of the recent attacks. These are the latest such incidents in a string of more than 40 similar ones around the country.

ANOMALI PINPOINTS PHISHING SCAM TO STEAL GOVERNMENT PROCUREMENT CREDENTIALS

The Anomali Threat Research team discovered a separate plot to steal login credentials from government workers operating in various countries around the globe in December 2019. The perpetrators placed false ads on fake government procurement websites, on which companies place bids to win contracts. These businesses have already registered with governments, enabling the hackers to skim their login data when they sign in to the illegitimate site.

The group is currently unidentified, according to Anomali, but the false websites' domains appear to be registered in Romania and Turkey, and the countries targeted included Australia, Canada, Mexico, South Africa, Sweden and the U.S. The hackers are also operating a pair of fake international courier websites to

steal similar data, though Anomali noted that the campaign is currently dormant.

FRAUD TRENDS AND DEVELOPMENTS

20 PERCENT OF STREAMING VIDEO AD REQUESTS ARE FRAUDULENT, STUDY FINDS

Fraud is seeing continued growth outside government-related scams, with a recent survey from television advertising agency MadHive finding that approximately 20 percent of all over-the-top (OTT) ad requests are fraudulent, up from 18 percent in March 2019. Overall ad spending totaled $3.8 billion for the year, meaning approximately $1.4 billion was lost to fraudulent OTT ads. Ad spend is projected to reach $5 billion in 2020, which will result in more wasted funds if ad request fraud continues to rise.

The largest contributing growth factor is that such fraud can be incredibly difficult to monitor. Nearly 40 percent of OTT ads are distributed using server-side ad insertion, which delivers ads directly from the streaming server and is much harder for advertisers to track than client-side ad platforms, which deliver ads from third-party servers. This allows fraudsters to issue false ad requests without advertisers realizing it.

ONLINE PAYMENT FRAUD SEES 9 PERCENT YEAR-OVER-YEAR INCREASE

The American Express 2019 Digital Payments Survey found that retail fraud was also on the rise last year, with 27 percent of online retail sales reported as fraudulent — up from 18 percent in 2018. Approximately 77 percent of retailers reported fraud in 2019, according to the study, and 42 percent of consumers experienced at least one attempt to fraudulently use their credit cards or other payment information.

The good news is that merchants are increasingly aware of the threat fraud presents, with 69 percent of retailer respondents spending significant time and money on payment fraud prevention. Consumers are also recognizing fraud risks: 59 percent were concerned about their payment information being compromised when making online purchases.

NEW ACCOUNT FRAUD RISES 18 PERCENT IN 2019

There has also been an upswing in new account fraud, which sees bad actors opening new accounts on websites and committing fraudulent activity within 90 days. A recent study found that this fraud type increased by 18 percent year over year in 2019, bringing its growth since 2014 to a staggering 108.6 percent. Experts attribute this to the prevalence of stolen identities on the dark web, which vastly increased in the wake of massive data breaches at Facebook, First American Financial and Verifications.io. These identities are available for as little as $15 apiece and often include selfies and driver's licenses.

New account fraud appears to have decreased slightly in recent weeks, despite its overall growth. A holiday fraud report found that the Black Friday-Cyber Monday holiday shopping weekend saw a 19 percent decline in such schemes. Fraud detection methods are also growing more popular, with the related market expected to skyrocket from $20 billion in 2018 to $80 billion by 2025.

ONLINE SCAMS HAVE AFFECTED 90 PERCENT OF AMERICAN CONSUMERS, SURVEY FINDS

A recent survey that MoneyGram commissioned found that 90 percent of Americans have been victims of some sort of fraud, including online scams, data breaches, identity theft or social media hacks. Scams such as fake romantic propositions and money transfer requests were the most common, at 63 percent. Fifty-six percent of respondents reported having been defrauded and 54 percent said their social media accounts were hacked.

Many respondents admitted to engaging in risky online behaviors that raised their probability of being victimized. One in 10 answered phone calls or emails from unknown origins, for example, while one in eight responded to unsolicited romantic requests.

AUSTRALIA'S 2019 FRAUD LOSSES DROP 5 PERCENT

Fraud is also a problem abroad, but it is receding in certain countries. Australia's total fraud losses for the 2018-19 financial year totaled $455 million AUD ($316 million USD), a 5 percent decline from the previous fiscal year's $479 million AUD ($333 million USD). AusPayNet, the country's premier payments fraud monitoring body, attributed the decline to a crackdown from the Reserve Bank of Australia, which threated banks and credit card providers with harsh regulations if the fraud rate did not decrease. Payment data tokenization and the Commonwealth Bank of Australia's (CBA) introduction of Apple Pay, which encouraged many Australians to use more secure payments platforms, were also factors. The CBA also instituted location tracking for mobile purchases, allowing it to more accurately flag fraudulent transactions.

UK CARD FRAUD ACCOUNTS FOR HALF OF EUROPEAN TOTAL

Digital fraud occurs in every nation, but not all are equally affected. A recent study from data analytics company FICO found that card fraud losses in the U.K. totaled £671 million ($882 million USD) in 2018, or slightly less than half of the €1.6 billion ($1.79 billion USD) recorded in Europe, Russia, Turkey and Ukraine combined. Most of the U.K.'s fraud losses resulted from card-not-present (CNP) fraud, which is largely conducted via online channels.

The U.K. figure represents a 19 percent increase over the previous year, which experts are attributing to changes in reporting and the growing availability of personal information online as a result of data breaches. The British government is employing various tools to fight this rise, including sending police officers to public schools to warn students about online fraud.

COMPANIES AND GOVERNMENTS FIGHT BACK

EASI, ADYEN PARTNER AGAINST PAYMENTS FRAUD

Companies are doing their part to protect themselves and their customers from fraud-related incidents, and that includes collaborations to bolster their defenses. Payments platform Adyen has partnered with food delivery company Easi to optimize the latter's payments process and secure it against various fraud types. Easi will integrate Adyen's RevenueProtect platform into its operations, leveraging its machine learning (ML) capabilities to identify fraudulent card testing and CNP fraud efforts. The platform also prevents false

positives by using algorithmic matching, behavioral analytics and device fingerprinting.

Online food delivery is a popular target for fraudsters, according to Evan Li, Easi's chief information officer. A 2019 report found that the food and beverage industry experienced a 79 percent year-over-year increase in fraud attacks in 2018 — a concerning number given that the report estimated that the value of mobile orders will reach $38 billion this year. Li noted that Adyen's products balance anti-fraud efforts and frictionless payment experiences and that its customizable risk rule engine has also reduced chargebacks — another common friction point with mobile ordering.

INDIAN GOVERNMENT CONSIDERS REGULATING SOCIAL MEDIA MARKETPLACES TO PREVENT FRAUD

India's Ministry of Consumer Affairs is considering regulations for selling products and services via social networks like Facebook, Instagram, Pinterest and WhatsApp due to increases in related fraud. The goal is for the networks' eCommerce platforms — such as Facebook Marketplace and WhatsApp Business — to operate under the same rules as other similar entities. WhatsApp has more than 400 million Indian users, and Facebook has 250 million. This prevalence has resulted in 46 percent of local poll respondents being scammed on one of these networks. Eighty-five percent of those polled expressed support for new eCommerce rules and policies.

DEEPDIVE

FRAUDSTERS GO PHISHING

Businesses have good reason to be concerned about data breaches. Fraudsters' attempts to access systems and steal valuable information are becoming more innovative, and research suggests they are also increasingly successful. Cybercriminals' accomplishments come at the expense of targeted businesses, with a recent study finding that individual data breaches cost firms around the globe an average of $3.92 million in 2019 — a 1.5 percent increase from 2018. The same report found that the total cost of a data breach had risen 12 percent since 2014.

Growing attack-related expenses force businesses to remain vigilant against emerging threats, including phishing and other fraud types that their own employees may willingly or unwillingly perpetuate. Another recent study found that phishing accounts for 90 percent of all data breaches and that such schemes increased 65 percent over the past year.

Businesses need employees to build and promote their products, but they cannot afford to have those workers weaken their security, meaning fraud prevention must be among firms' top priorities. The following Deep Dive delves into the steps companies can take to ensure their employees are knowledgeable about phishing and are at the front lines of anti-fraud efforts.

FIGHTING THE PHISHERS

Phishing attempts threaten many firms' security operations, often tricking employees into revealing email addresses, login credentials, passwords or other sensitive details. Workers could receive emails that appear legitimate but contain links that request such details, and fake vendors, fraudsters impersonating trusted contacts or malware could manipulate users into giving away information.

One notable phishing attack occurred in 2015, when healthcare giant Anthem suffered a breach that compromised more than 80 million patient records. The scheme originated from a number of phishing emails that targeted a handful of employees. Anthem paid out $16 million in a class action lawsuit, underlining how a relatively minor phishing attempt can have catastrophic consequences for businesses and their customers.

Companies can ensure protection by educating employees, running them through scenarios, adopting cybersecurity measures that filter out nefarious websites and implementing policies that require passwords to meet complexity standards and be frequently updated. Two-factor authentication (2FA) or encrypting sensitive data can also help.

ENSURING SECURE WORKPLACE PRACTICES

Other fraud attempts targeting workplaces are no less dangerous. A changing workforce filled with more remote and non-traditional gig employees opens new doors for criminals looking to steal sensitive information. Workplace lapses can enable cybercrime, and some workers might not realize how their everyday actions endanger their companies. A survey from document destruction company Shred-It found that 25 percent of employees leave their computers unlocked and unattended, which could grant fraudsters access when employees step away, for example. Those who write passwords or important notes on paper present similar opportunities, enabling bad actors to snap photos and log into secure systems.

Remote work is becoming a point of concern as it becomes more common. Many employers believe off-site employees represent significant vulnerabilities, but they do not ensure these workers are taking protective steps. Most surveyed small and medium-sized businesses (SMBs) said they do not have related policies in place, despite the fact that fraudsters can use unsecured Wi-Fi connections at homes or coffee shops to target these employees, thus endangering company data and resources.

The gig economy represents more than one-third of the total U.S. economy, but freelance and contract workers may not have to follow the same obligations as full-time employees. Companies can address these security gaps by updating policies to require clean desks and other specific expectations for remote workers. Such rules may also compel in-house employees to lock sensitive details in desk drawers, shred paper documents and responsibly dispose of computer hardware. They should also know whom to contact if a computer, laptop or phone is stolen.

Remote workers require their own protocols to ensure they do not fall victim to fraud. Data from gig worker marketplace Upwork found that while 63 percent of firms hire remote employees, 57 percent do not have remote work policies to ensure security. Companies should craft remote worker guidelines that clarify these rules and include secure resources, like video and phone conference lines, project management services and cloud-based document platforms, to ensure off-site and in-house employees use the same offerings. Every employee should also have access to a company contact in the event of a suspected breach.

Employees are the backbone of any company's success, but businesses must ensure they are not used against them. Preparedness can go a long way toward enabling workers to remain vigilant on the front lines against phishers and other fraudsters, especially as traditional work shifts away from offices.

about

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

DataVisor's mission is to build and restore trust online. It partners with the largest financial and internet properties in the world to protect them from a wide array of attacks, including fraud, abuse and money laundering. The company's unsupervised ML-based detection solution detects attackers without needing training data, and often before they can do damage.

DataVisor is made up of a team of world-class experts in Big Data infrastructure and ML. It builds advanced algorithms to fight the world's most sophisticated online attackers.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at **digitalfraud@pymnts.com**.

disclaimer

The Digital Fraud Tracker® may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.