ADAPTING TO NEW FRAUD CHALLENGES
TABLE OF CONTENTS

1- HOW COVID IMPACTED THE FRAUD LANDSCAPE
2- DATA BREACHES
3- AUTHENTICATION
4- PHISHING
5- MALWARE
6- LOOKING AHEAD
ADAPTING TO A NEW NORMAL

COVID-19 drastically changed the ways in which people were accustomed to working and conducting business. Adapting to a new “new normal,” meant that organizations were faced with a unique set of challenges.

FIRST ADOPTING NEW TECHNOLOGIES

In order to ensure that employees could fully conduct their jobs remotely, organizations had to implement new tools and software to protect sensitive data.

SECOND AN ONLINE EXPERIENCE

In order to provide the same services to all customers remotely, organizations had to quickly adopt a fully digital platform.

A TARGET FOR ATTACKERS

The need and urgency to adopt fully digital platforms was the perfect opportunity for malicious actors to launch targeted schemes.

Fraud schemes were especially effective because of the opportunity that COVID provided. One of the most popular scams is related to vaccines and COVID cures. Approximately 22,000 new COVID related domains were registered in a matter of weeks claiming to sell protective equipment, sanitizers, and medications to treat the virus.

Approximately 18 million malware and phishing emails and more than 240 million COVID-19 related spam messages are sent over Gmail daily.

The FBI names some of the most popular and effective fraud schemes seen in the last year:

• Government Impersonators
• Fraudulent Cures or Medical Equipment
• Work-from-Home Fraud
• Investment Fraud

These attacks will continue to evolve and grow as the pandemic runs its course.
APPROXIMATELY 18 MILLION MALWARE AND PHISHING EMAILS AND MORE THAN 240 MILLION COVID-19 RELATED SPAM MESSAGES ARE SENT OVER GMAIL DAILY.
IBM reports $3.86 million as the average cost of a data breach in 2020.

It was a busy year for cybercriminals as there were roughly 3,950 data breaches. About 80% of these occurring due to stolen credentials, or brute force attacks.

A LOOK AT SOME OF THE BIGGEST BREACHES THIS LAST YEAR:

MARRIOTT
The Marriott breach was disclosed March 31, 2020 and it impacted nearly 5.2 million customers who use the hotel chain’s loyalty program. It was a result of hackers obtaining credentials of two employees who had access to sensitive customer data.

MGM RESORTS
In July 2020 MGM Resorts was affected by a data breach that compromised about 142 million guest credentials. The information compromised included customer names, emails, physical addresses, phone numbers and dates of birth.

ZOOM
They say every action has a fraudster reaction. With the heavy reliance on virtual platforms like Zoom, it’s no surprise they faced a data breach in 2020 resulting in 500,000 compromised credentials.

CARNIVAL
Carnival Cruise Lines experienced a breach due to a ransomware attack in August 2020. Fraudsters stole confidential information of customers, employees, and crew members at the time of the attack.

The vast number of compromised credentials makes the username/password combination an ineffective method for safeguarding sensitive data. Especially in the Marriott breach which was a direct result of hacked employee credentials. There needs to be a more secure way to authenticate users.
IT'S TIME TO KILL THE PASSWORD

There are various factors that can be used to authenticate users, yet most organizations rely heavily on the use of passwords. It’s time to eliminate the password altogether and implement strong authentication.

THE EVOLUTION OF AUTHENTICATION

PASSWORD: The first password-based system was created in the early 1960s at MIT, meaning that the password is more than five decades old; multiple lifetimes in the tech world. Even then, it wasn’t secure. We know this from one of the researchers first using the system who was only allotted four hours of use per week, which wasn’t enough to run his tests. So, he hacked the master list of passwords stored on the system in order to be able to use more of the computer system’s time. Clearly, passwords have never been synonymous with security.


DEVICE RECOGNITION: Cookies were created in the late 1990s and became very mainstream in the early 2000s. They were the first example of widespread device recognition. Since then, the technology has evolved and improved to include a variety of methods that are constantly being updated.

SMS OTP: These began to be used widely in the early 2000s, and marked the beginning of passwords in general being delivered to phones (eventually through email and later soft tokens).

PUSH: Push notifications were first used by Blackberry, but Google and Apple took them mainstream in 2009 and 2010.

FINGERPRINT BIOMETRICS: TouchID from Apple in 2013.

QR: Whatsapp web launched in 2015.

FACE BIOMETRICS: FaceID in November 2017 from Apple.
Evolved from physical biometrics, behavioral biometrics identifies users through patterns such as mouse and keyboard movements, usage preferences, and hand-steadiness.

Behavioral biometrics continuously measures user activity to constantly ensure that a person is who they say they are, using data such as mouse use characteristics like press-size and time, and keystroke motions such as speed and style.

Behavioral biometrics is incredibly powerful—but it’s just one piece of data about incredibly dynamic users.

There are many more data points that can offer context about users. Behavioral biometrics tells you someone is clicking around on a desktop, but can it tell you their computer’s operating system, browser version, IP address, location, or time of day? This is where contextual data must come into play.

Contextual analytics allows you to understand if a user is who they say they are based on the device they’re using, when/where they are accessing sensitive data from, among other things.

A model that combines both behavioral biometrics with contextual device analytics can be up to 91% accurate for static authentication.

The anti-fraud industry is moving towards a holistic view of users as it realizes that no single solution is strong enough on its own—including biometrics.
Phishing has been around for decades and shows no signs of disappearing anytime soon. With low operational costs, minimal technical knowledge required, and a high return on investment, criminals continuously turn to phishing to make profits. The COVID-19 pandemic provided fraudsters with a platform to launch new targeted attacks.

**The Facts:**

Based on Appgate's global incident reporting there has been a rise in users victimized by phishing attacks by 345% from December 2019-December 2020. This can be partly attributed to the COVID-19 pandemic and speaks to the significance of a strong anti-phishing strategy.

22% OF DATA BREACHES INVOLVED PHISHING.

NEARLY 30% OF CONFIRMED PHISHING PAGES (APPROXIMATELY MORE THAN A QUARTER OF A MILLION) PERTAIN TO COVID-19 ALONE.

PHISHING ATTACKS ACCOUNT FOR MORE THAN 80% OF REPORTED SECURITY INCIDENTS.

MOST SECURITY INCIDENTS OCCUR AS A RESULT OF INFORMATION BEING COMPROMISED, WHICH MAKES PHISHING THE FIRST STEP IN THE FRAUD LIFECYCLE.

**Largest Targets for Phishing**

APWG's Phishing Activity Trends Report gives an overview of the industries that were most targeted in 2020.

**Most Targeted Industry Sectors**

<table>
<thead>
<tr>
<th>Industry Sector</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS/Webmail</td>
<td>31.4%</td>
</tr>
<tr>
<td>Financial Institution</td>
<td>19.2%</td>
</tr>
<tr>
<td>Payment</td>
<td>13.4%</td>
</tr>
<tr>
<td>Social Media</td>
<td>12.6%</td>
</tr>
<tr>
<td>Commerce</td>
<td>7.2%</td>
</tr>
<tr>
<td>Logistics/Shipping</td>
<td>4.2%</td>
</tr>
<tr>
<td>Telecom</td>
<td>3.2%</td>
</tr>
<tr>
<td>Cloud Storage/File Host</td>
<td>2.1%</td>
</tr>
<tr>
<td>Other</td>
<td>6.7%</td>
</tr>
</tbody>
</table>

**Keep in Mind**

As more anti-phishing security measures are put in place, we see an increase in highly sophisticated attacks. Their targeted nature makes them much more dangerous and effective.

**Out with the Old**

Traditional security strategies are no longer effective to combat the evolving threat landscape. It is imperative to implement a multilayered, intelligent fraud protection strategy that is constantly adapting to new and advanced threats.
STAY ON GUARD

It is now common to find multiple malware families working together in complex infection chains, creating even more effective attacks.

Attacks are becoming more and more capable of lateral movement through victims’ networks, making it difficult to get rid of the infections.

IT’S ALL ABOUT RANSOMWARE

Ransomware is the second most common type of malware next to Password Dumper.\(^{17}\)

In a recent survey, more than half of all respondents said their organizations had been through a ransomware attack in the last year and cybercriminals were successful in encrypting data in 73% of these attacks.\(^{16}\)

According to cyber security experts, ransomware attacks have increased 40% to 199.7 million cases globally as of Q3 of 2020.\(^{18}\)

Victims of the 11 biggest ransomware attacks have spent around $144.2 million in recovery related to these attacks.\(^{20}\)

This breakdown from Lumu’s ransomware flashcard demonstrates the percentage of companies affected by ransomware:\(^{21}\)

- NORTH AMERICA – 69%
- LATAM – 61%
- EUROPE – 57%
- MIDDLE EAST & AFRICA – 61%
- APAC – 55%
FRAUD IN CONSTANT MOTION

Every day, malicious actors develop new tactics to uncover and target any potential weak points in security infrastructures. Organizations must keep pace by evaluating existing fraud prevention strategies against the ever-changing fraud landscape.

VISIBILITY IS KEY

One of the key elements to preventing attacks and protecting your organization is visibility. Understanding when and how your organization has been targeted is key to mitigating the effects of an attack.

WHERE THERE’S AN ACTION, THERE’S A FRAUDSTER REACTION

Institutions must take their strategies to the next level and strive to not only keep pace with the evolution of fraud but to also stay a step ahead of malicious actors by anticipating up-and-coming threats and possible vulnerabilities found on devices or networks. Only then can security and anti-fraud teams enhance their strategies to take advantage of the latest and greatest industry tools.

There are wide range of options and technologies on the market, but at the end of the day, simply being aware of each organization’s unique environment and needs is what will help teams determine and implement the strongest approach for combatting present and future fraud.
11. https://www.wired.com/2012/01/computer-password/
Appgate's secure access solutions enable digital businesses with a security strategy that reduces risk, removes complexity and instills the confidence needed to move forward. Appgate provides a layered protection strategy across the multi-step fraud lifecycle.

WWW.APPGATE.COM