STAYING AHEAD OF THE EVOLVING THREAT LANDSCAPE
# Table of Contents

- Introduction .................................................. 3
- A closer look at the top three attack types
  - Phishing .................................................. 5
  - Stolen credentials ........................................ 8
  - Ransomware .............................................. 9
- On radar: Mobile attacks ................................... 10
- Getting ahead of the curve ................................. 12
As cybercrime and fraud goes, 2021 was filled with more of what we’ve seen in the past ... phishing, ransomware, malware attacks and more. 2022 is no different, but these types of attacks are evolving with increased sophistication and improved targeting as fraudsters leverage machine learning and AI.

And “here-to-stay” remote workforces greatly expand attack surfaces that create additional opportunity for targeting organizations and consumers alike. Getting ahead of these attacks can be challenging as scammers use new strategies.

At Appgate, we conducted our yearly Faces of Fraud survey in conjunction with ISMG. The results provided insightful information about different attacks and which fraud schemes are most concerning to various financial services organizations.

**HERE ARE SOME HIGHLIGHTS AROUND HOW FACES OF FRAUD SURVEY RESPONDENTS EVALUATED THE THREAT LANDSCAPE IN 2021.**

- When asked about the number of fraud incidents and losses in the last year, 81% of respondents noted that the number of fraud incidents has remained steady or increased
- 78% of respondents indicated that anti-fraud controls are now seen as a more desired customer feature in digital platforms
- 38% believe today’s fraud schemes evolve too quickly to keep pace
According to the published 2021 Data Breach Investigations Report by Verizon, these are three methods used to carry out cyberattacks in 2021:

- **Phishing**
- **Stolen credentials**
- **Ransomware**

If one thing has remained the same throughout the last few years, it’s that the people of any sized organization remain the most vulnerable and easily exploitable attack vector.
Phishing or social engineering is here to stay. It requires minimal technical knowledge, is easy to scale and users continue to fall victim due to the increased sophistication of these attacks. Attackers have tailored attacks to appear more realistic using company logos, branding and more.

There is still a belief that only affluent markets and organizations are the ones being targeted, but the reality is that cyberattacks have no boundary nor do they discriminate against emerging markets and their organizations.

### HOW PHISHING HAS IMPACTED ORGANIZATIONS GLOBALLY

- Phishing became a top breach type during COVID-19 as more employees began working from home.
- Phishing attacks account for more than 80% of reported security incidents.
- 74% of organizations in the U.S. have experienced a successful phishing attack.
- According to APWG, the number of phishing attacks has tripled from early 2020.
- Phishing is the number one cause of enterprise cybersecurity breaches and has been for the last two years, with 43% of total incidents involving phishing.
- Phishing attacks can cause losses to the tune of $17,700 per minute and are among the leading cyberthreats.
Another form of social engineering is known as vishing (an acronym for Voice Phishing). Vishing is a type of scam carried out by criminals through telephone calls with the aim of obtaining a person’s personal or banking data. According to INCIBE (National Cybersecurity Institute from Spain), the cases of vishing have been steadily increasing, and in Latin America many of these calls are made from prisons.

SIM swapping involves duplicating the SIM card of a smartphone. The SIM (Subscriber Identity Module) card in a cell phone stores the customer’s access code and the telephone company’s telephone number. The danger of SIM swapping is that it is not necessary to physically access a mobile device to duplicate a SIM card. For this purpose, criminals contact the customer service of telephone operators and pose as legitimate users. They thus hijack the victim’s phone line and use all their information to, for example, request new passwords and receive verification codes in order to access their online banking service.

With the increasing use of QR codes due to the pandemic and the progressive return to the new normal (e.g., on restaurant menus), this mechanism has become a favored attack vehicle to hide fake URLs, which is a modality better known as QRishing.

According to Phishing Insights 2021 global survey, phishing attacks increased 61% in Mexico.

Particularly in the Peruvian region:
- 6 out of 10 Peruvians do not recognize messages that may be a cyber-scam
- 61% of Peruvians do not know what malicious messages are
- 40% of phishing attacks are financial in nature
- For identity fraud 80,000 people are victims of scams and provide personal information to cybercriminals
- Since 2019, the SIM swap fraud has considerably grown in Latin America, becoming one of the main digital security threats in the region
- According to surveys from the mobile phone industry, 4 out of 5 attempts to change a chip are successful

According to a report from the Anti-Phishing Working Group, phishing attacks in December 2021 were up to 316,747, which was the highest since the APWG has been keeping track. The number of attacks tripled since 2020.
TOP INDUSTRIES TARGETED BY PHISHING ACCORDING TO THE APWG:

Social Media: 11.0%
E-commerce/Retail: 13.1%
Logistics/Shipping: 3.5%
SaaS/Webmail: 29.1%
Telecom: 3.5%
Financial Institution: 17.8%
Payment: 7.1%
Crypto: 5.6%
Other: 9.3%

PHISHING CAN NEGATIVELY IMPACT AN ORGANIZATION’S REPUTATION AND CAUSE SIGNIFICANT FINANCIAL LOSS. LUCKILY, THERE ARE WAYS TO AVOID ATTACKS AND PROTECT YOUR ORGANIZATION AND CONSUMERS.

STRATEGIES TO AVOID PHISHING ATTACKS:

• Consumer and employee awareness
  - Ensure that your employees and customers are aware of what phishing is and how it can be avoided. Inform them of the latest trends and advise them to look out for suspicious emails that may contain malicious links.

• Round-the-clock phishing monitoring
  - Protect your organization against phishing attacks by having some type of continuous monitoring solution that identifies, reports, and quickly removes phishing sites on your behalf before they become a more serious threat to your organization.
  - A strong anti-phishing solution should report the type of phishing impacting your organization and exactly how so that you may take action accordingly.
Credentials remain one of the most valuable and sought-after data types, and this pattern will continue. The motivation for the use of stolen credential is 100% for financial gain.

Hackers prefer to go after stolen credentials as this could easily open the door to full access into any organization’s network. According to the Verizon 2021 Data Breach Investigations Report, 61% of data breaches stem from leveraged credentials and 25% of the breaches was from this stolen data.

The deep dark web is full of stolen credentials allowing easy access into any organization infrastructure. In many instances these credentials are utilized across other platforms, which would allow easy entry when being used with credential stuffing tools.

**BEST APPROACH TO PROTECT YOUR CREDENTIALS:**

- Never share your credentials with other parties
- Always have different passwords for each account/login
- In the eventuality of a data breach, all passwords in the organization must be reset
- Strong password is very important
- Multi-factor authentication has been proven to be a great layer of security
- Behavioral biometrics is proving to be a formidable safety net
Ransomware is by far the most prolific and publicized threat facing organizations today. These attacks are incredibly difficult to recover from. As malicious actors increase the stakes in their attacks, organizations are forced to pay more and more to gain access to their sensitive data. Even with payment, there’s no guarantee that any of these files will be recovered.

Ransomware is a multiple step process for threat actors, beginning with phishing and credential theft. Reducing external phishing threats and ensuring access is secured makes an immediate impact. It is just as essential however to ensure privilege escalation is minimized, preventing lateral movement of the actor and their malware. Fight phishing, practice good credential hygiene and adopt a Zero Trust mindset to stop ransomware.

**NOTABLE 2021 RANSOMWARE ATTACKS**

- **JBS** – Food Processing Company
- **Colonial Pipeline** – Oil Company
- **Kronos** – Workforce Management Company
- **Kaseya** – Software Company

**THE IMPACT OF RANSOMWARE IN 2021:**

- Ransomware attacks cost an average of **$4.62 million**, more expensive than the average data breach ($4.24 million) ¹⁰
- Compromised credentials were the most common initial attack vector, responsible for **20% of breaches** ¹¹
- Ransomware costs are expected to reach **$265 billion** by 2031 ¹²
- There were over **700 million ransomware attacks** in 2021 alone ¹³
- During 2021 in Latin America, the average cost of a data breach was estimated at **$2.56 million dollars**, an increase **52% compared to 2020** (Cost of a Data Breach Report 2021 - IBM) ¹⁴
Mobile attacks. Malicious attacks have moved from desktop browsers and computers to mobile apps and devices, where end users now spend much of their time online. Cybercriminals are leveraging security vulnerabilities, SMS phishing, QRishing and a myriad of other techniques to infect mobile devices and steal the sensitive data needed to compromise accounts.

Staying ahead of these trends is of utmost importance considering the significant role mobile devices play in our daily lives. This is especially true for financial services organizations considering the myriad of P2P applications frequently used by consumers daily.

It’s impossible to control or limit what your consumers do on their device. However, there are some ways in which organizations can reduce their mobile risk exposure.

MALICIOUS ACTIVITY ACROSS THE MOBILE CHANNEL:

- Verizon’s Mobile Security Report states that 50% of companies “are falling behind attacker’s capabilities,” and 54% of companies were “less confident about the security of their mobile devices than that of their other systems”15

- Verizon’s report also states that 48% of survey respondents said that their organization had experienced a mobile-related compromise with major effects, and 63% of those said that the repercussions were lasting 16

- In the 2021 Faces of Fraud survey, 41% of respondents noted a rise in fraud affecting the mobile channel 17

- 23% of Faces of Fraud survey respondents also noted a rise in creation of fraudulent accounts (customer onboarding) via the mobile channel

- Mobile malware attacks are increasing, with 156,710 mobile banking trojans identified in 2020 alone 18

- As two-factor authentication has become more prevalent, fraud behavior is shifting to emerging countries where the use of smart devices is not as prevalent within the general population, thus bringing a lower level of protection
ON RADAR: MOBILE ATTACKS

HOW TO APPROACH MOBILE RISK:

• Similar to phishing, employee and consumer education is paramount. **Ensure your customers** know how to spot malicious texts and how to ensure they are using a secure device.

• The most effective approach is to implement a security strategy that focuses on assessing risk. **A truly exhaustive mobile fraud protection solution must be capable of assessing whether a device is risky** (by being jailbroken, for example). It should allow organizations to decide which devices should be denied access based on their risk tolerance.

• It’s especially important to offer **increased protection to customers of financial institutions** who do their banking via smartphone or tablet.

• **Align your mobile protection capabilities** with your whole fraud prevention strategy by leveraging device security analytics to create more robust risk detection models and make them more dynamic.
Getting ahead of the curve. With the state of cybersecurity constantly evolving in the face of geopolitical challenges, global health crises and the rise of nation state actors, here are some answers on how to get ahead in 2022.

**IN OUR 2021 FACES OF FRAUD SURVEY, WE ASKED RESPONDENTS TO CHOOSE THEIR BIGGEST CONCERNS FOR 2022. THEY WERE:**

- Account takeover: 45%
- Phishing: 42%
- Business email compromise: 36%

**WE ALSO ASKED ABOUT FRAUD PREVENTION TOOLS THAT THEY PLAN TO INVEST IN FOR THE NEXT YEAR, HERE’S WHAT THEY HAD TO SAY:**

- Artificial intelligence/machine learning: 41%
- Multifactor authentication: 31%
- Fraud detection and monitoring systems: 27%
- Transaction monitoring: 27%
Protecting your organization may seem overwhelming, especially considering the various techniques and threats, but there are a few things you can do to ensure peace of mind.

A STRATEGIC APPROACH TO IMPLEMENTING CYBERSECURITY SOLUTIONS

- It’s important to cover all your bases when it comes to protecting your organization. Protecting the company itself is of the utmost importance, but it’s equally important to have security solutions that protect employees and customers accordingly.
- Some organizations have the resources and expertise to be able to mitigate any cybersecurity threat, but there are many other organizations that very quickly get overwhelmed by cybersecurity mitigation efforts. This is understandable as sometimes this is not their core expertise. For this we highly recommend seeking guidance from the cybersecurity experts who are involved in the day-to-day cybersecurity effort.

STAY INFORMED

- Understanding the fraud/threat landscape is the first step to implementing a strong cybersecurity strategy across your organization.
- Every action has a fraudster reaction. We’ve seen this with the pandemic. Fraudsters used that opportunity to launch additional fraud schemes targeting the people during a time when there was much uncertainty and misinformation. Many fell victim to these attacks because of that. Understanding how these events can impact cybercrime is important when trying to stay ahead of the curve.

EDUCATE EMPLOYEES AND CONSUMERS

- Constant training and awareness for employees and consumers. Cybersecurity is always dynamic and in constant evolution.
- Employees and consumers can help augment your cybersecurity defenses by knowing what to look out for in terms of cyberattacks.
- See something, say something. Set up an abuse box where customers and employees can forward potentially malicious emails, texts or websites. This can help your organization rapidly identify targeted threats and act accordingly.
SOURCES

1) The 2021 Faces of Fraud Survey
2) Verizon 2021 Data Breach Investigations Report
3) Verizon 2021 Data Breach Investigations Report
4) Security Boulevard: Preparing for Evolving Phishing Scams
5) Security Boulevard: Preparing for Evolving Phishing Scams
6) APWG Phishing Activity Trends Report
7) Security Boulevard: 10 Phishing Stats that’ll make your c-suite think
8) Security Intelligence: Phishing Attacks Are Top Cyber Crime Threat, Easier Than Ever to Create and Deploy
9) 9a & 9b
   b. APWG Phishing Activity Trends Report
12) Forbes: More Alarming Cybersecurity stats for 2021
13) Toolbox: 700M Attacks om 2021 and Counting: Can Businesses Fight the Ransomware Tsunami?
16) Mobile Security Index 2021
17) The 2021 Faces of Fraud Survey
18) SC WHY any new financial ‘Super App’ needs bulletproof security
Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.