Anticipated fraud trends for 2021

By Cathie Webb and Shannon Weber

As a supplier of employee management software, we are sadly aware of some of the payroll and related fraud which takes place in business. Tough economic times mean that the temptation to commit a "small" fraud become more tempting than ever.

We need to be aware, and to take any possible precautions against fraud, both in business, and in our personal capacities.

1. Data breaches will continue to be bigger than ever, with new technologies used for malicious reasons. The more confusion caused, the more fraudsters use this to their advantage to steal data, details of valuable online accounts and money.

2. Across the world, governments and agencies have failed to create strong, trusted identity management solutions, which means that synthetic IDs and pure identity theft will continue to increase, especially as banks and credit grantors continue to neglect reporting these losses or lose them in credit losses. We will see continued attacks on central infrastructures that manage digital address books for immediate payment accounts.

3. Account takeover techniques will move to the next level. As more and more of our daily lives takes place online, the value of digital accounts increases. While account takeovers (ATO) are nothing new, we'll see an explosion of techniques used to steal login credentials.

   This is a problem across all verticals and while organisations spend millions on preventing chargebacks and transaction fraud, ATOs aren't taken as seriously as they should be –by merchants and fraud prevention teams.

   This perfect storm gives fraudsters access to increasingly sophisticated tools to illegally access the data transferred to a website, including login and password details, scraping for ATO's.

Even multiplying authentication methods isn't as safe as it once used to be, as bypassing 2 factor authentication (2FA) becomes ever more sophisticated.

4. Phishing will evolve dangerously. Organisations and individuals are losing valuable assets without giving away passwords, by falling for seemingly legitimate text messages or email requests. Those who take the bait, end up forwarding a digital token, which gives fraudsters indefinite access to all their cloud data, including emails, files and contacts – even after the victim changes their passwords. Phishing is still the number one cause for data breaches, with more than 35% of the major data breaches started with phishing techniques.

   Over the past years, phishing techniques from hackers and fraudsters have included the creation of fake job posts, to obtain the applicants' personal data, and collecting phone numbers for SIM jacking, which results in multiple accounts takeovers.

   More than ever before, companies and individuals will need to ensure they are vigilant at all times, to avoid giving away information that could hurt them – especially if they want to avoid embarrassing and reputation-damaging data breaches.

5. The European Union's 2nd Payment Services Directive (PSD2) and open banking will continue to transform the online landscape. FinTech's and established financial institutions were the first verticals to feel the changes brought on by the PSD2. The world of ecommerce is undergoing transformation as SCA (strong customer authentication) is gradually rolled out across Europe. Unfortunately, this will probably create a period of customer confusion. As new services provide OTPs (one-time passwords) via SMS, 2FA and MFA, and even more app-based biometric authentication methods, fraudsters will try to exploit the lack of consumer information to fool users into submitting valuable data.

   Periods of change are fruitful for fraudsters, as we have seen with previous implementations of new techniques like Chip and Pin or the abuse of Captcha forms. The new security methods could also impact conversion rates, as providing a seamless user experience is the new battleground for online businesses, whether it's for onboarding or for completing transactions.

   Adding an extra step between customers and their purchases has already proved controversial with certain retailers. On the flipside, banks and fintech's alike are enthusiastic about the new opportunities of open banking. According to FData 80% of large banks want to support fintech application development through open banking. FinTech's also welcome the opportunity to scale by partnering with established financial institutions thanks to the brand recognition they will provide.

6. ID theft and synthetic ID fraud will target new services. New security measures often increase customer confusion, which opens the door to data theft. A good example would be the new rules from the Gambling commission, which forces users to provide ID scans upfront.

   The problem is that these measures, while born from good intentions, create a massive demand for stolen and synthetic IDs. These bad IDs are used to target the payday and fast loan industries, and the size of that market is bound to increase in 2021.

Links, References and Notes

Accsys, a division of Transaction Capital Transactional Services (Pty) Ltd. provides people management solutions i.e., Payroll, Human Resources (HR), Time and Attendance as well as Access Control/Visitor Management.
The company develops, implements, trains and services our solutions. We provide readers, turnstiles, booms and CCTV. We run both on premise and in the cloud, as well as mobile options for ESS. Recruitment, online education and Business Process Outsourcing (BPO) are part of our offering, too.

www.tctransactionalservices.co.za
http://www.tctransactionalservices.co.za
www.accsys.co.za
http://www.accsys.co.za
email: cathie.webb@accsys.co.za
twitter: @CatiWeb

Comcorp has, for the past 26 years, focused on solving business challenges in the financial services sector, by developing proprietary software solutions. Comcorp has developed an innovative toolkit which enables businesses to effectively and compliantly onboard customers, whilst mitigating their risk of processing fraudulent transactions.

www.comcorp.co.za
https://www.comcorp.co.za/secure-payslip-exchange/
email: shannon@comcorp.co.za

References:

https://s3.amazonaws.com/cfsi-innovation-files-2018/wp-content/uploads/2020/08/20170608/FHN_Kresge-Report_final.pdf
http://www.treasury.gov.za/comm_media/press/2020/WB081_Fintech%20Scoping%20in%20SA_20191127_final%20(002).pdf
https://seon.io/resources/the-top-5-fraud-trends-for-2020/