Looking back at 2020 to see how social engineering evolved during the pandemic and how it's developing in 2021.

Social engineering in 2021

kaspersky

Adapting to a new normal

2020 was an unprecedented year. As large swathes of the world's population were forced into one form of lockdown or another, our lives changed forever. The internet became our workplace, our classroom, where we shop and conduct business. It also became a lifeline as the only means to keep in touch with loved ones. In response, businesses had to rush their digital transformation efforts, delivering in a matter of weeks what would normally have taken years, with varying degrees of success. Combined with the inevitable financial crisis, many businesses were forced to shut down and some industry sectors, such as hospitality and non-food retail, were particularly affected. On the other hand, digitally native businesses and those that could still innovate in the face of adversity were better able to weather the storm, from restaurants becoming digital takeaways to grocery stores converting to online ordering and delivery in a matter of weeks, to name but a few. This is when "working from home" (#WFH) replaced all previous nomenclature around "flexible working" and Zoom became a verb[1].

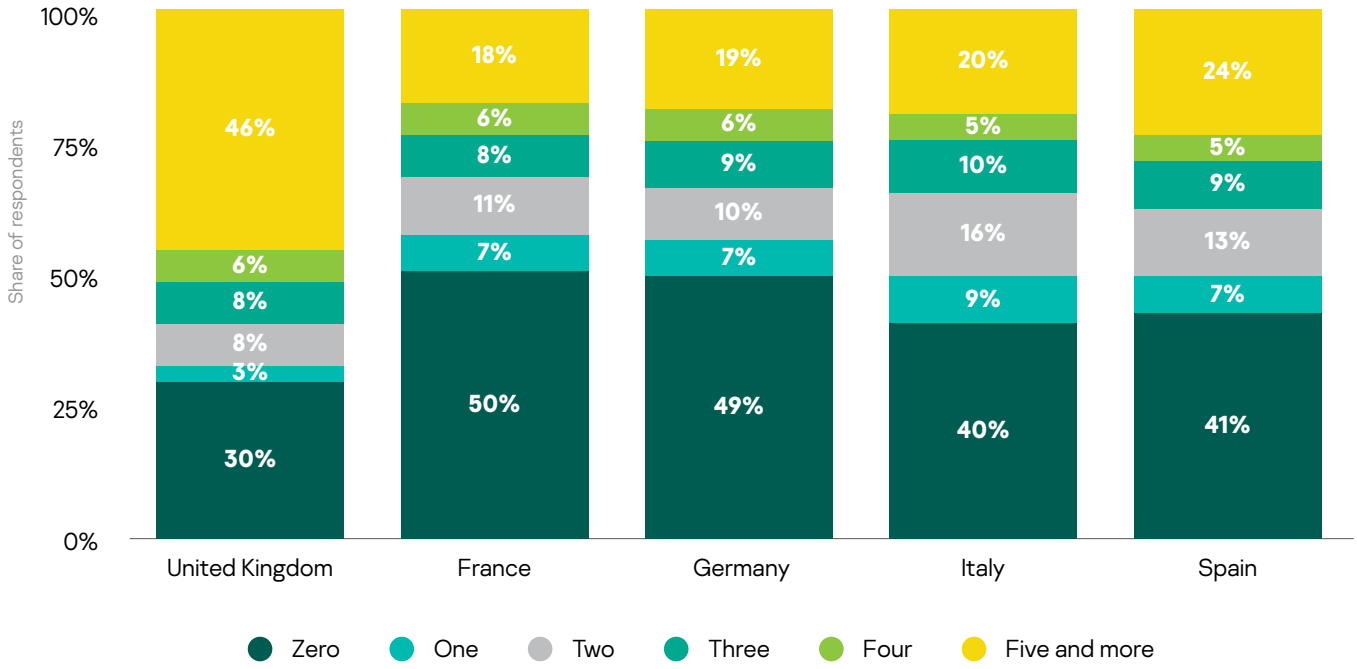


Figure 1 Statista 2020[2]

The challenging economic conditions also meant that many lost their jobs. New employment trends emerged, such as increased participation in the gig economy, and many of those previously in traditional full-time employment were forced to pursue gig or temporary work for supplementary or even primary income. Governments also had to scramble new digital processes to manage the healthcare and financial crises, either by launching contact tracing apps, or by finding ways to deliver financial stimulus or benefits packages without excluding segments of the population.

[1] https://www.bbc.co.uk/news/business-52884782

[2] https://www.statista.com/statistics/1142519/coronavirus-working-from-home-in-europe/

Changing behaviors

Younger generations were traditionally at the forefront of digital adoption, but the pandemic also changed that. By necessity, older demographic segments – often technology averse – acquired new behaviors, as evidenced by the increase in first-time users across the spectrum of digital services[3]:

Digital adoption rate, by industry[1]

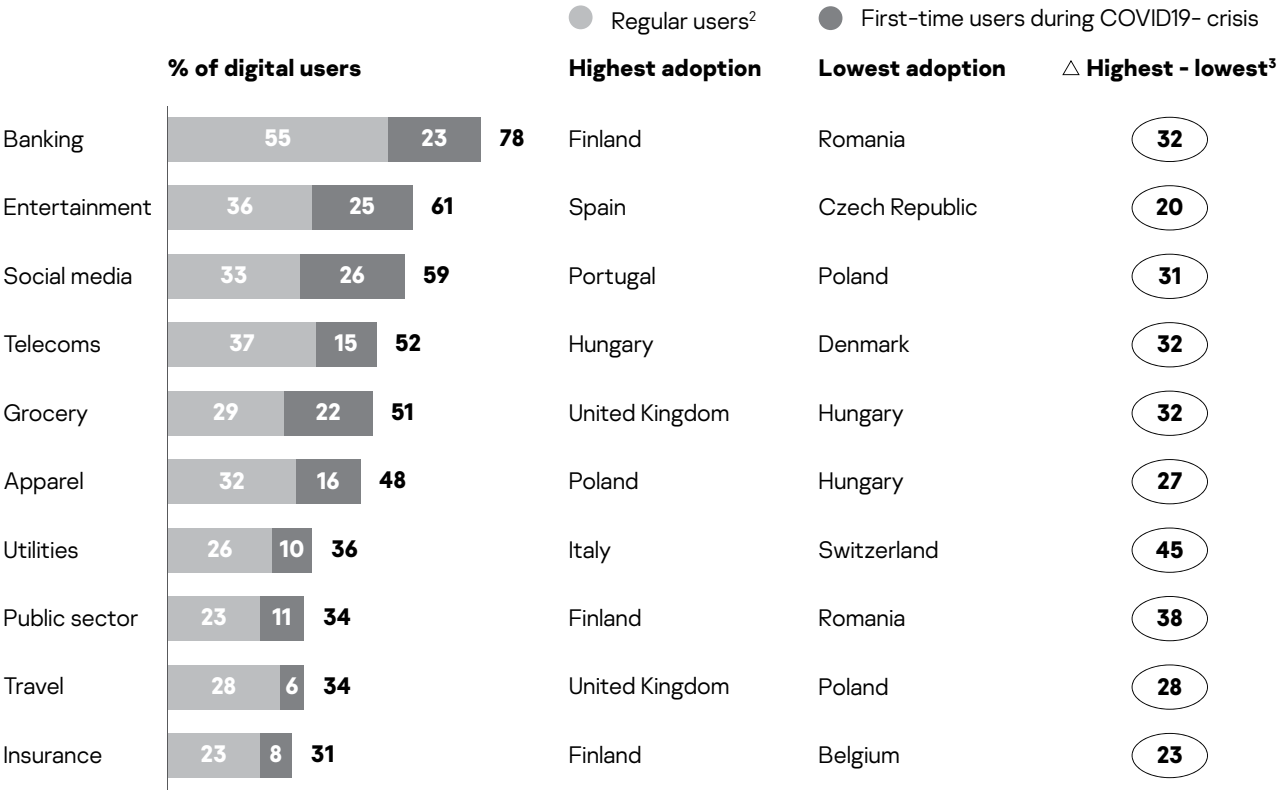


Figure 2 McKinsey 2020[4]

For individuals, this increased, often forced, digitization, has brought new risks which are difficult to address given the pace of adoption. Unsurprisingly, according to the last FBI Internet Crime Complaint Center (IC3) 2020 Internet Crime Report[5], the older you are, the more you have to lose:

2020 VICTIMS BY AGE GROUP

Victims		
Age Range	**Total Count**	**Total Loss**
Under 20	23,186	$70,980,763
20-29	70,791	$197,402,240
30-39	88,364	$492,176,845
40-49	91,568	$717,161,726
50-59	85,967	$847,948,101
Over 60	105,301	$966,062,236

As for organizations, they were forced into changing their working practices, with many more people – often in positions of trust – working from home or other remote locations, they were faced with the challenge of ensuring that the comparative safety of the "corporate infrastructure" was replicated in this often unfamiliar "distributed infrastructure" where the distributed locations were than 1,000 sensitive files open to every member of staff[6]. For criminals, compromising employees can lead to an exceptional bounty....

[3] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-COVID-19-recovery-will-be-digital-a-plan-for-the-first-90-days#

[4] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/europes-digital-migration-during-covid-19-getting-past-the-broad-trends-and-averages

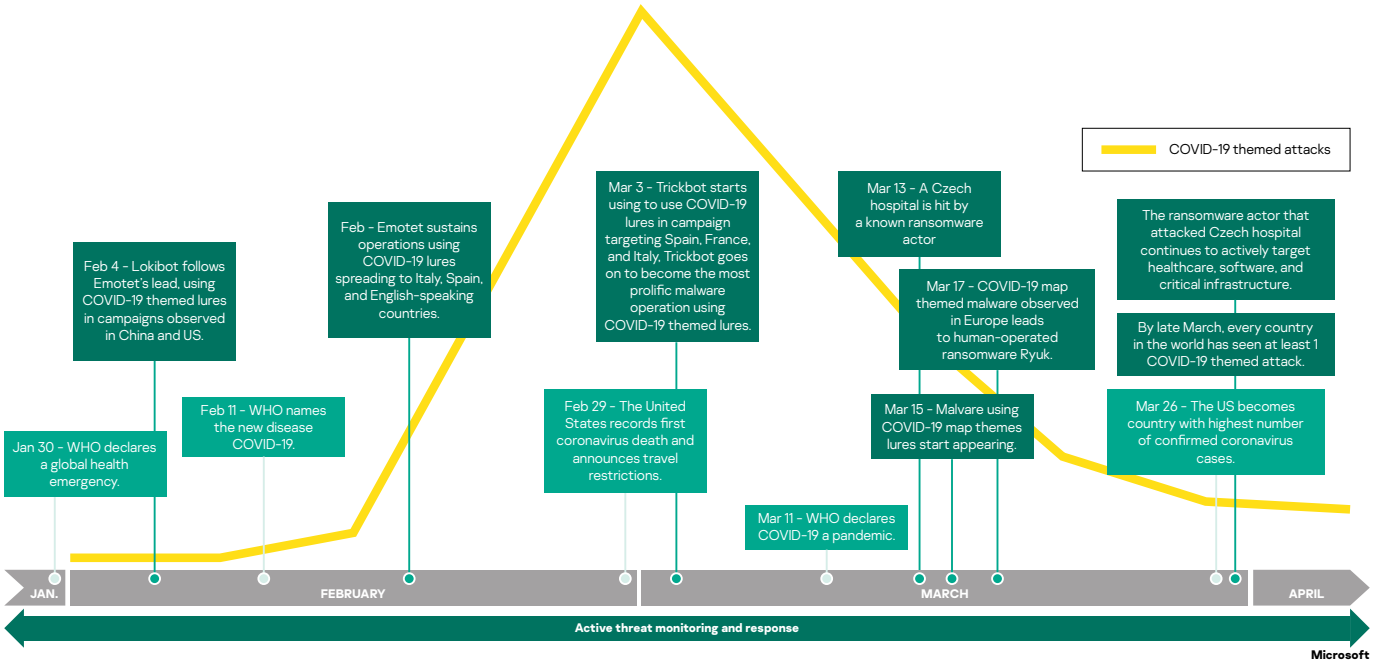
[5] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[6] https://www.computerweekly.com/news/252492132/Financial-services-data-volumes-heighten-risk-of-insider-breach

For many companies, the changes deployed in 2020 were only the first steps on this necessary journey. Outdated processes required re-modelling, machine learning models needed to be re-evaluated[6], and new or exacerbated risks required adequate mitigation. Not unexpectedly, major risks linked to increased cybercrime fraud emerged during the first year of the pandemic. Consequently, cybercrime cost the world $1 trillion in 2020[7].

The perfect melting pot

It is understood that hackers will always capitalize on crises to launch opportunistic attacks, and COVID-19 was no different. Sure enough, as soon as the World Health Organization named the global health emergency "COVID-19", attackers started to actively deploy opportunistic campaigns, taking advantage of local events and news (indeed, the WHO itself was targeted[8]):



Both Google and Microsoft performed extensive research on the effects of the pandemic on online security threats[9] [10], and the consensus is that criminals capitalized on the need for information for both businesses and individuals as the crisis evolved. However, the global malware trends remained fairly stable and criminals merely repurposed their existing infrastructures lures and malware to geographical circumstances: whilst we observe an opportunistic peak in COVID-19 themed attacks in early March, this soon settled into a new normal (and COVID-19 has just become one other lure amongst many). As criminals continued to social engineer their way into businesses to deliver their payloads, compromise infrastructures and harvest credentials to commit further crimes, some industries were more affected than others.

[6] https://www.finextra.com/newsarticle/37534/bank-machine-learning-models-hit-hard-by-covid

[7] https://www.itproportal.com/news/cybercrime-cost-the-world-over-dollar1-trillion-in-2020/

[8] https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC

[9] https://blog.google/threat-analysis-group/findings-covid-19-and-online-security-threats/

[10] https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

No honor amongst thieves

Sadly, as the crisis evolved, criminals targeted key industries and several ransomware groups that had already compromised multiple infrastructures, mostly through social engineering, activated numerous ransomware deployments in April 2020. And because the pandemic was an opportunity not to be wasted, they specifically focused on healthcare, aid organizations, medical billing companies, manufacturing, transport, government and educational institutions, with no regard to the devastating human impact[11]. Indeed, according to the IBM X-Force Report[12], nearly one in four cyberattacks last year was ransomware, while the increase in data extortion efforts – a new phenomenon – enabled one ransomware hacking group to make over $123 million in profits in 2020, especially targeting those organizations that couldn't afford downtime.

However, these critical sectors were not the only ones under threat, and not even those that suffered the most: healthcare was only the seventh-most targeted sector in 2020, up from last place in 2019. In second and third places respectively, the manufacturing and energy sectors were specifically targeted during the pandemic, mostly as a result of industrial control systems (ICS) and legacy environment vulnerabilities[13].

Not unexpectedly, the finance and insurance industry topped the list of most-attacked for the fifth year in a row (IBM X Force), as the pandemic created the perfect environment for financial fraud to thrive. Experian dubbed COVID-19 "the gateway to fraud"[14] and identified the five most prominent threats in 2020:

- Authorized push payment (or wire transfer) fraud (BEC, EAC)
- Account takeover fraud
- Account opening fraud
- Transaction payment fraud
- Synthetic identity fraud (also known as fictitious identity fraud)

And this is where most of the impact is felt: social engineering remains the most prominent way of committing crime by attacking not only businesses but individuals, as evidenced by the latest FBI/IC3 report:

2020 CRIME TYPES

By Victim Count	
Crime Type	**Victims**
Phishing/Vishing/Smishing/Pharming	241,342
Non-Payment/Non-Delivery	108,869
Extortion	76,741
Personal Data Breach	45,330
Identity Theft	43,330
Spoofing	28,218
Misrepresentation	24,276
Confidence Fraud/Romance	23,751
Harassment/Threats of Violence	20,604
BEC/EAC	19,369
Credit Card Fraud	17,614
Employment	16,879
Tech Support	15,421
Real Estate/Rental	13,638
Advanced Fee	13,020
Government Impersonation	12,827
Overpayment	10,988
Other	10,372
Investment	8,788
Lottery/Sweepstakes/Inheritance	8,501
IPR/Copyright and Counterfeit	4,213
Crimes Against Children	3,202
Corporate Data Breach Ransomware	2,794
Ransomware	2,474
Denial of Service/TDoS	2,018
Malware/Scareware/Virus	1,423
Health Care Related	1,383
Civil Matter	968
Re-shipping	883
Charity	659
Gambling Terrorism Hacktivist	391
Terrorism	65
Hacktivist	52

2020 CRIME TYPES CONTINUED

By Victim Loss	
Crime Type	**Loss**
BEC/EAC	$1,866,642,107
Confidence Fraud/Romance	$600,249,821
Investment	$336,469,000
Non-Payment/Non-Delivery	$265,011,249
Identity Theft	$219,484,699
Spoofing	$216,513,728
Real Estate/Rental	$213,196,082
Personal Data Breach	$194,473,055
Tech Support	$146,477,709
Credit Card Fraud	$129,820,792
Corporate Data Breach	$128,916,648
Government Impersonation	$109,938,030
Other	$101,523,082
Advanced Fee	$83,215,405
Extortion	$70,935,939
Employment	$62,314,015
Lottery/Sweepstakes/Inheritance	$61,111,319
Phishing/Vishing/Smishing/Pharming	$54,241,075
Overpayment	$51,039,922
Ransomware	**$29,157,405
Health Care Related	$29,042,515
Civil Matter	$24,915,958
Misrepresentation	$19,707,242
Malware/Scareware/Virus	$6,904,054
Harassment/Threats Violence	$6,547,449
IPR/Copyright/Counterfeit	$5,910,617
Charity	$4,428,766
Gambling	$3,961,508
Re-shipping	$3,095,265
Crimes Against Children	$660,044
Denial of Service/TDos	$512,127
Hacktivist	$50
Terrorism	$0

[11] https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware
[12] https://newsroom.ibm.com/2021-02-24-IBM-Security-Report-Attacks-on-Industries-Supporting-COVID-19-Response-Efforts-Double
[13] https://cybersecurity.att.com/blogs/security-essentials/how-covid-19-has-increased-vulnerabilities-in-industrial-control-systems
[14] https://www.experian.com/blogs/global-insights/covid19-as-a-gateway-to-fraud-top-5-global-fraud-trends-to-watch-out-for-in-2020/

The listed crimes are not new, and the trends continue to reflect what we already know: criminals will continue to capitalize on opportunities, and the pandemic gave them plenty. Whether through capitalizing on world events and local knowledge – as observed with the attacks on the healthcare extended supply chain and those associated with it – or on individuals suffering with the mental exhaustion brought on by the pandemic, as evidenced with the increase in phishing attacks and confidence fraud/romance scams. As the world becomes more secure, targeting individuals – whether in their personal lives or as employees of companies – is easier and far more lucrative than mounting "sophisticated" attacks on technology, and the rewards are potentially much higher. After all, if one individual is compromised and credentials are lost, criminals have the keys to the kingdom and don't have to worry about evading traditional technological security measures.

Because of the sheer volumes involved with a pandemic, criminals adapted rapidly to capitalize on their investments. This is why we saw the increase of ransomware-as-a-service, and the double-extortion tactics (i.e., ransom and then threaten to leak data) and any variations of corporate-like operating models (e.g., outsourcing part of the process to specialists in specific attacks). This was also facilitated by the increased use of cloud infrastructures, as numerous businesses that rushed into "digital" unwittingly left unsecure servers exposed for all to see....

Fighting back...

Looking back at 2020, we soon realize that there was nothing new. Granted, new industries and demographic segments were targeted, some attacks increased, but the ways criminals operated during the pandemic is no different to the way they have always operated when presented with the opportunity of a global event (e.g. the 2018 Olympics[15]). The kill chain remained the same:

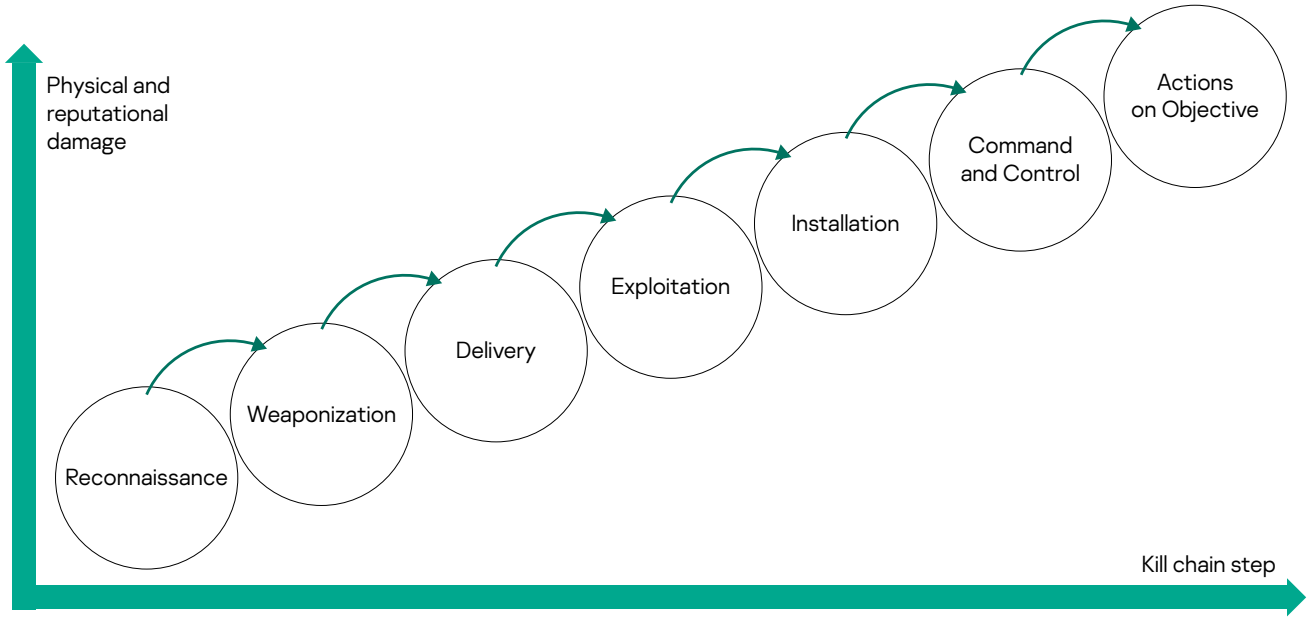


Figure 3: Attack lifecycle (kill chain)[16]

A large proportion of businesses were already compromised prior to the pandemic (e.g., payloads lying dormant), the pandemic gave criminals the perfect opportunity to complete the cycle. Furthermore, increased digitization and cloud adoption gave criminals the perfect opportunity to enact the kill chain even more rapidly by targeting newly digital businesses and individuals, where survival, not security, was the focus.

As businesses worldwide start to recover and stabilize their operations, moving from survival to sustainability, and as individuals see hope in the easing of lockdowns, one thing is certain: we will not go back to the way we were. Growth still presents a challenge, and digitization is here to stay. To maintain trust, businesses must now understand that their customers and partners not only have high expectations of convenience but equally high expectations for security[17]. And as we enter this next phase, the fundamental security principles remain the same as they always have been: deploy processes in line with the new normal, train people to recognize threats, and use technologies (and don't be afraid of new technologies) that best support the security posture. Of course, all this needs to be applied through the lens of confidentiality, integrity and availability.

[15] https://money.cnn.com/2018/02/09/technology/pyeongchang-olympics-cyberattacks-south-korea/index.html

[16] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07171449/Incident_Response_Guide_eng.pdf

[17] https://patch.com/michigan/farmington-mi/security-most-important-retaining-mobile-banking-customers

For example, the need for better authentication in all aspects of digital interactions has never been more pressing: whether looking at Privileged Access Management, Identity and Access Management, or Strong Customer Authentication or Zero Trust architectures, businesses should have a clear understanding of where they need to strengthen their environment.

Another example is combating phishing and other forms of social engineering. These are not new threats and should be well understood. Preventing phishing impersonation will mitigate the risk of brand impersonation, yet DMARC deployment globally is still not where it should be[18], and of course user training to recognize phishing interactions is crucial, as well as the appropriate governance processes to prevent scams such as APP and BEC.

When it comes to vulnerabilities, organizations would do well to always consider the OWASP Top 10[19], as well as the OWASP Top 10 Mobile[20], given the increase in digital and mobile usage worldwide.

The list of recommendations could go on, but it will not show anything new. The trick is to deploy a layered approach and manage risk according to the business appetite and circumstances.

Looking ahead...

According to Forrester[21], the following five threats could hobble recovery:

Misinformation and espionage: those in critical sectors such as government and healthcare and their supply chains should take advantage of industry and government threat intelligence sources to be prepared to counter this risk.

Insider threats: as the world moves towards recovery, there will be many employment casualties. As organizations move more and more towards digital operations and government relief packages peter out, redundancies are to be expected as businesses are forced to make tough decisions. This will leave many employees disgruntled as they face unemployment and these could turn into insider threats. Businesses are advised to deploy the appropriate governance processes and technologies that could prevent this from happening.

Identity theft and account takeover: this risk, whilst not new, is expected to continue on its upward trajectory as digital interactions continue to increase. Businesses are advised to consider deploying or enhancing the measures highlighted in the previous section.

Bot attacks: criminals use technology too, and to make their operations more efficient, they will use means to automate their processes. Bot attacks have been on the rise for the past couple of years and this trend will continue. Attacks such as inventory hoarding, credential stuffing, ad fraud, and web scraping will continue to rise and businesses are advised to deploy preventative measures.

COVID-19 apps: contact tracing apps and immunity passports will be particularly at risk in 2021 as they become mainstream. Those involved should deploy best practices in information security and data privacy to counter this threat.

[18] https://www.prnewswire.com/news-releases/scammers-target-wall-street-in-new-capital-call-fraud-schemes-reveals-investigation-by-email-security-firm-agari-301239190.html

[19] https://owasp.org/www-project-top-ten/

[20] https://owasp.org/www-project-mobile-top-10/

[21] https://www.techrepublic.com/article/forrester-these-5-threats-could-hobble-pandemic-recovery/

Fortunately, current regulatory developments have driven enhanced security globally, such as seen with PSD2 in Europe and the various data protection and Anti-Money-Laundering regulations worldwide. In the UK, the fight against APP fraud is under way, with the adoption of the Contingent Reimbursement Voluntary Code of Conduct (an initiative to reimburse victims) which has gained traction beyond the original signatories[22] as well as the continuing deployment of Confirmation of Payee. In addition, technology giants are under increasing pressure to fight scams and protect victims[23 24 25]. Increased cooperation can only be a good thing. In addition, many businesses are now adopting layered approaches to counter these threats. With the relentless increase in digital interactions, more and more focus is placed on the customer experience, and businesses must ensure that these experiences are not only seamless, but secure. Customers no longer feel safe with passwords[26], and multi-factor authentication is gaining a lot of traction, with biometrics now part of life[27]. But as interactions become more immediate, the need for real-time visibility has led to even additional factors such as physical biometrics (e.g. face recognition, fingerprints, etc.) to being increasingly supplemented by more contextual features such as behavioural biometrics and analysis (e.g. typing behaviour, page interaction, etc.), contextual device and environment analysis and the likes. Luckily, technology innovation doesn't just serve criminals.

Be prepared...

The pandemic brought with it increased digitization and increased risks. But examining attack patterns, we soon realize that it is nothing we haven't seen before. Granted, there is more technology to take advantage off, there are more opportunities presented to criminals, but we know how to address these risks. The only difference perhaps is, as technology advances, there are many more ways to counter threats than ever before. Let's take advantage of these innovations within tried and tested risk management and governance processes, and apply common sense. That will go a long way....

[22] https://www.lendingstandardsboard.org.uk/registered-firms/#contingent-reimbursement-model-code-crm-for-authorised-push-payment-scams

[23] https://www.ft.com/content/4a356d66-9b05-4666-9b16-9f8e73abe565

[24] https://www.finextra.com/newsarticle/37752/mps-slam-action-fraud-fca-and-tech-giants-over-pension-scams

[25] https://www.telegraph.co.uk/news/2021/03/23/scammers-running-riot-tech-giants-allow-adverts-rogue-firms/

[26] https://www.businesswire.com/news/home/20210407005308/en/Consumers-No-Longer-Believe-Passwords-Are-the-Most-Secure-Method-for-Authentication

[27] https://www.biometricupdate.com/202104/consumers-recognize-biometrics-security-tops-passwords-experian-says

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

kfp@kaspersky.com