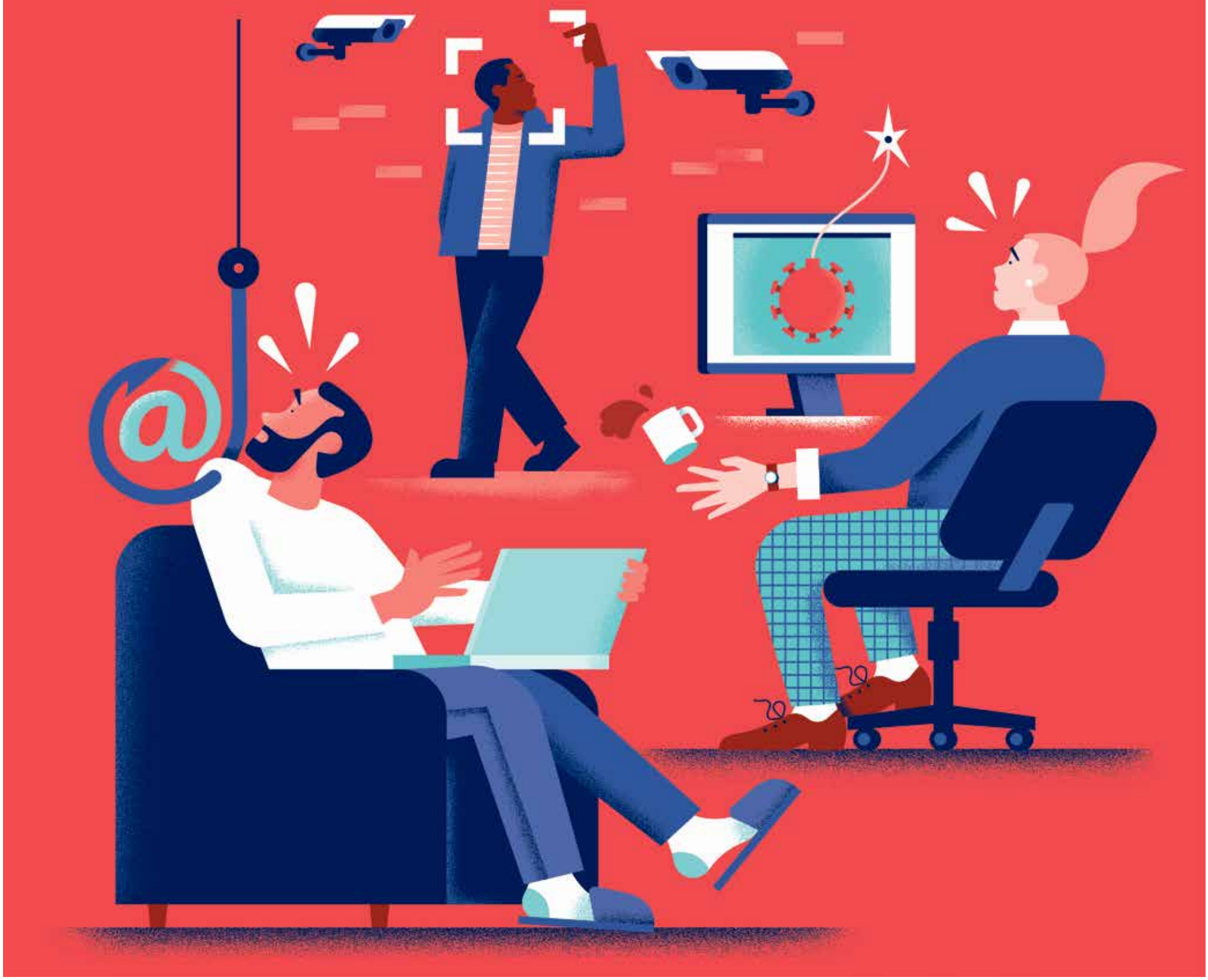
FRAUD & PRIVACY



ONLINE BUSINESS ACCOUNTS AND PAYMENT PROCESSING THAT DO MORE

One-stop solution for banking and online payment processing

Multi-currency business accounts

Integrated Fraud and Privacy solutions

www.safenetpay.com

safenetpay

FRAUD
& PRIVACY

Distributed in
THE TIMES

raconteur reports

Publishing manager
Helen Glynn

Associate editor
Peter Archer

Deputy editor
Francesca Cassidy

Managing editor
Benjamin Chiou

Digital content executive
Taryn Brickner

Head of production
Justyna O'Connell

Design
Sara Gelfgren
Kellie Jerrard
Harry Lewis-Irlam
Celina Lucey
Colm McDermott
Samuele Motta
Jack Woolrich

Art director
Joanna Bird

Design director
Tim Whitlock

@raconteur /raconteur.net @raconteur_london

raconteur.net fraud-privacy-2020

CYBERCRIME

Leaving the door open for fraud

Cybercriminals thrive on uncertainty and a global pandemic couldn't be better for causing worry, disrupting normal business processes and creating opportunities for disgruntled employees

Chris Stokel-Walker

Cybercriminals are opportunists. Seeing opportunity, they attack and one of the biggest opportunities to commit fraud is a global pandemic upturning the world in every way possible. The old ways of doing business have been overhauled in an instant; in many cases, the office itself has disappeared. Chaos and confusion have reigned, opening the door for fraud.

Phishing attacks increased by 667 per cent in March alone, as criminals seized their opportunity. As a result, awareness of fraud and privacy has never been more important. "Everything that's new is going to have a new security angle we hadn't thought of," says Dr Eerke Boiten, professor of cybersecurity at Leicester's De Montfort University. "How that's going to be exploited is going to be interesting."

The fault lines are obvious and plentiful, and criminals are scurrying through the cracks. Remote working is one major area ripe to be exploited. More business is being transacted by email and the number of spear phishing attacks is on the rise. One wrong click, or the opening of a suspicious attachment in error, can result in a breach of privacy and the potential for enormous fraud against organisations.

"We've seen, and will continue to see, scams and frauds that exploit disruption," says cybersecurity expert Jessica Barker. Preying on fears, such as messages purporting to be from a firm's human resources department, informing staff members that a colleague has tested positive for the coronavirus and should click on an attachment outlining procedures, is one way into networks and has already victimised at least one Canadian company.

But there are far greater risks than employees being out of the office, out of sight and therefore out of mind. The gradual return to workplaces worldwide is itself a potential vector for fraud, says Barker, who believes employees could easily field phone calls from scammers pretending to be in-house IT support asking for passwords to get access to systems.

The broader economic disruption, with a quarter of UK workers furloughed and tens of millions worldwide unemployed, provides another way to commit fraud.

JUSTIN TALLIS/AFP via Getty Images

There's the potential for supplier impersonation stemming from disruption to the norms of business. For example, fraudsters could send emails or make phone calls to companies claiming that the normal contact at a firm has left their job, asking them to change key details, including where they pay invoices.

"The whole point of spear phishing and social engineering is to force people to make quick decisions, possibly by perturbing their normal situation a bit," says Boiten. "We're already in that situation, doing unusual things all the time now." Coupled with the fear of acting quickly to address any issues, and an attempt to catch up on lost business, the opportunity to crack open the door and enter a business's systems fraudulently has theoretically never been easier.

Companies who would ordinarily be in the business of receiving goods and delivering services to others may have to scramble to seek alternative sources for the original product to be able to deliver their services to clients, potentially overlooking due diligence and falling into fraud traps. "Everyone is worried," says Barker. "This all creates a perfect storm for cybercriminals to seek to exploit."

It's not just current staff members being hoodwinked that managers and their IT department need to be wary of. Insider threats are also a real risk, with people within organisations potentially being more likely to cause problems. We know economic uncertainty and unemployment is a driver of increased crime in general and cyber-fraud is no different.

"A lot of people are feeling uncertain, upset and have financial worries. Some may feel it's unfair their pay is frozen," says Barker. "All these feelings mean the risk of malicious insiders may be higher."

Some may be doing so for personal gain or the ability to take advantage of hesitancy around illnesses. One American employee of a Fortune 500 company told his boss he had tested positive for COVID-19, though he hadn't been affected by the virus. He supplied a hospital letter he had faked for the purpose.

The company, fearing the worker could have contaminated the workplace, quarantined a plant, advised some of his closest colleagues to self-isolate and spent more than $100,000 to do so. Federal prosecutors charged the man in May with defrauding his employer.

The FBI has also warned businesses to be on the lookout for employees trying to take advantage of the pandemic. The Insurance Fraud Bureau has cautioned insurance fraud is likely because of the economic hardship the coronavirus is wreaking.

Others may be willing to siphon off data from inside and give it to competitors or trade it on illicit online markets. Insider fraud, with a particular focus on the disclosure of internal processes to facilitate fraud, is one of the major concerns raised by the Fraud Advisory Panel, a UK industry body, alongside phishing emails and the subsequent compromise of business accounts.

Compulsion is often driven by disgruntled employees who feel wronged by businesses, which could be an issue when people are returning to work in a high-stress situation and being asked to do more with less support.

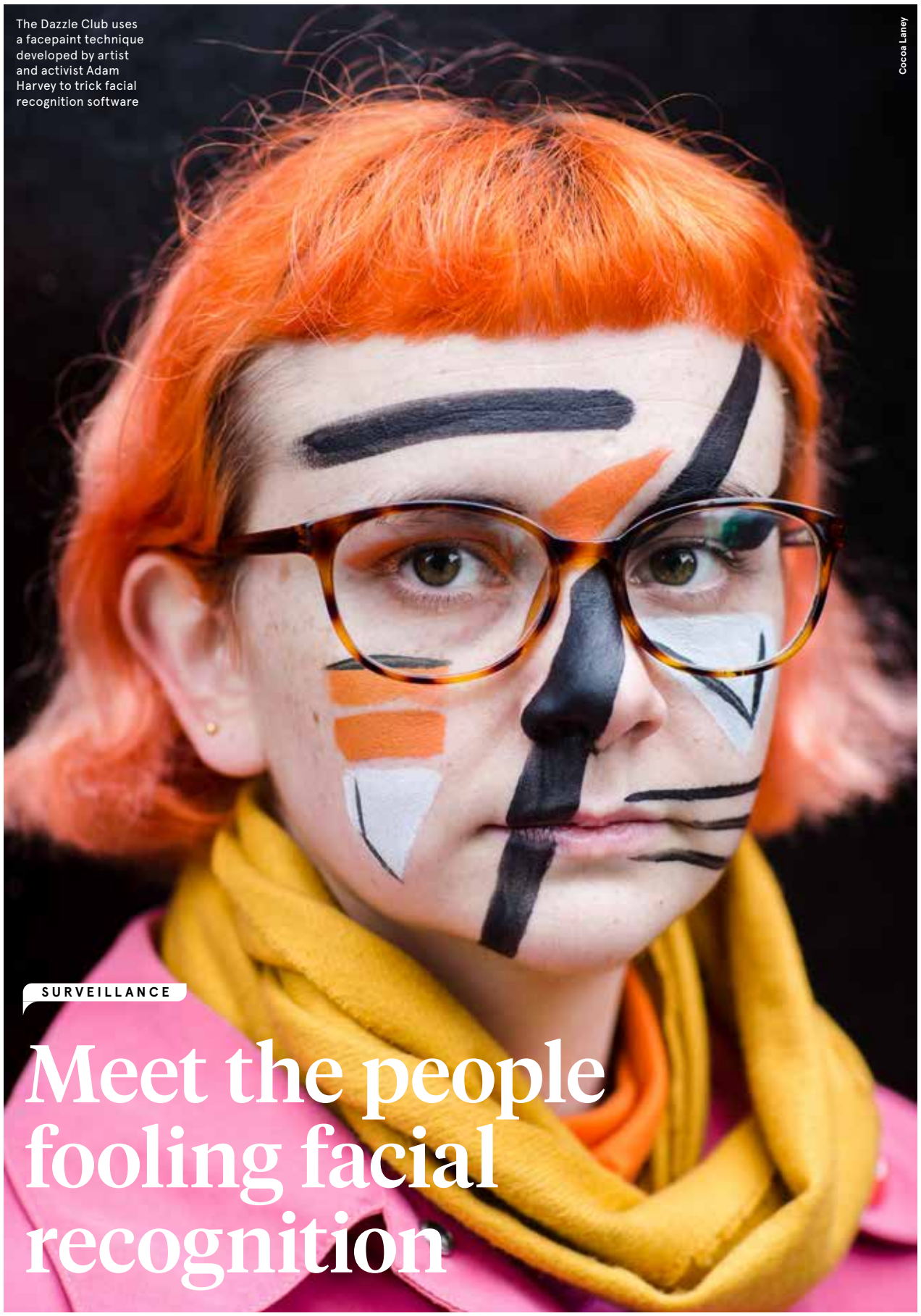
Trying to help employees feel less distant and alone is more vital than ever and making sure they feel willing to come forward if tricked by an outside attacker is crucial. "When people are potentially still working from home, and if they click a link in an email or download something or transfer money, they don't have a colleague to turn to and ask what to do, so there's a danger we might not know about incidents," Barker concludes.

1 in 10
URLs are malicious

1 in 412
emails sent are identified as malicious

1 in 3,207
emails are phishing emails

Symantec/Broadcom 2019



The Dazzle Club uses a facepaint technique developed by artist and activist Adam Harvey to trick facial recognition software

Cocoa Laney

SURVEILLANCE

Meet the people fooling facial recognition

Activists are finding ways to get around facial recognition software as the debate around ethical surveillance rages on

Sam Haddad

A decade ago, it was possible to attend a protest in relative anonymity. Unless a person was on a police database or famous enough to be identified in a photograph doing something dramatic, there would be little to link them to the event. That's no longer the case.

Thanks to a proliferation of street cameras and rapid advances in facial recognition technology, private companies and the police have amassed face data or faceprints of millions of people worldwide. According to Big Brother Watch, a UK-based civil liberties campaign group, this facial biometric data is as sensitive as a fingerprint and has been largely harvested without public consent or knowledge.

In response, designers and privacy activists have sought to make clothing and accessories that can thwart facial recognition technology. According to Garfield Benjamin, a post-doctoral researcher at Solent University, who specialises in online privacy, they rely on two main techniques.

"Either they disrupt the shape of the face so that recognition software can't recognise a face is there or can't identify the specific face," he says. "Or they confuse the algorithm with different patterns that make it seem like there are either hundreds or no faces present."

At the University of Maryland, Tom Goldstein, associate professor in the Department of Computer Science, is working on the second technique. He's created a so-called invisibility cloak, though in reality it looks more like an incredibly garish hoodie. The cloak, a research tool which is also sold online, works by fooling facial recognition software into thinking there isn't a face above it.

In 2015, when Scott Urban, founder of Chicago-based privacy eyewear brand Reflectacles, saw facial recognition becoming "more popular and intrusive", he set out to make glasses that would "allow the wearer to opt out of these systems".

He created a model designed to block 3D infrared facial scanning, used by many security cameras, by turning the lenses black. While another model reflects light to make it harder to identify a user's face data from a phone picture.

Other anti-surveillance designs include a wearable face projector, which superimposes another face over that of the person wearing the device, a transparent mask with a series of curves that attempts to block the facial recognition software while still showing the user's facial expressions, balaclavas with a magnified pixel design and scarves covered in a mash up of faces.

Benjamin says the problem with all these techniques is that the companies making the facial recognition technology are always trying to improve their systems and overcome the tricks, often boasting in their promotional literature about the anti-spoofing mechanisms they are working on. "They want to show they're thwarting the 'rebels' or 'hackers' and this has led to further developments in the technologies," he says.

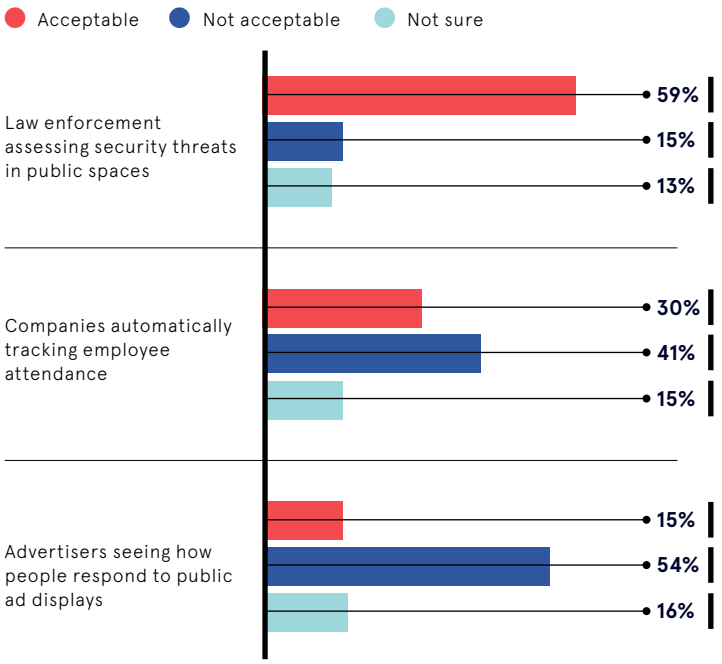
This was the case with CV Dazzle, which uses face paint to trick or dazzle the computer vision by disrupting the expected contours, symmetry and dimensions of a face. The technique was invented by the American artist and activist Adam Harvey in the early-2010s and it proved to be effective at confusing the software that was emerging at the time, though it's creator has noted it doesn't always fool present-day tech.

Yet, it does still disrupt the facial

> **It's about making that invisible tech visible... especially as the Met Police are starting to deploy these cameras in the city**

PUBLIC ATTITUDES TOWARDS FACIAL RECOGNITION

Share of US adults who find the use of facial recognition acceptable/not acceptable in the following situations



Pew Research Center 2020

Reflectacles

Right: The IRpair glasses by Reflectacles are designed to block 3D infrared facial scanning

tagging of some social media, according to Georgina Rowlands of The Dazzle Club, a UK-based privacy activist group inspired by Harvey. "We know the technique is still effective versus Facebook, Snapchat and Instagram's algorithms," says Rowlands, whose group lead monthly walks, adorned in their rather striking Bowie-esque face paint, around London to explore privacy and public space in the 21st century. "But we haven't been able to access more advanced systems such as the Metropolitan Police's, so we can't say if it's effective there."

But evading the tech is only part of the story for The Dazzle Club. It's as much about raising awareness of the pervasiveness of facial recognition software. As another member of the group Emily Roderick says: "It's about making that invisible technology visible and bringing out those discussions, especially as the Met Police are starting to deploy these cameras in the city."

The real goal for many of these creators is regulation of facial recognition technology companies and those who use the faceprints, to protect the privacy rights of the individual. So whether someone is at a protest or simply walking down the street, they can trust that their face, and all the data contained within it, remains their own and theirs alone.

Qilai Shen/Bloomberg via Getty Images

Exploring the future for facial recognition development

In the wake of the Black Lives Matter protests, IBM, Microsoft and Amazon announced they would no longer be allowing US police departments to access their facial recognition technology, for at least a year.

The tech is arguably a tool of racial oppression. In 2018, Joy Buolamwini, a researcher at the MIT Media Lab, and Timnit Gebru, a member at Microsoft Research, showed that some facial analysis algorithms misclassified Black women almost 35 per cent of the time, while nearly always getting it right for white men.

A further study by Joy Buolamwini and Deborah Raji demonstrated that Amazon's Rekognition tool had major issues identifying the gender of darker-skinned individuals, but made almost no errors with lighter-skinned people.

Raji, who is a tech fellow at the AI Now Institute at New York University and an expert in computer vision bias, explains there are many ways in which facial recognition technology can be biased. "It could involve having a higher error rate for a minority group," she says. "Or it could label members of a particular group with a problematic label, so for example predicting people of colour are angrier than white or other people."

Algorithmic flaws, which can be caused by a poor and narrow dataset, or inherent in the algorithm design itself, can have major repercussions for an individual. "Once you're in the system, it's very easy for the system to identify you in a variety of poses and angles, but the threat of being misidentified is quite large and, should that happen, you're going to face real-world consequences."

This was the case for Robert Julian-Borchak Williams, who was wrongly arrested in front of his children and detained for 30 hours due to a faulty facial recognition match. Even without such high-profile mistakes, several studies have shown there is no compelling evidence that facial recognition technology is actually effective in policing.

The backlash to facial recognition software chimes with a public weariness about how much they can trust police institutions, according to Raji. "Because of that, we're thinking should we be giving them this power to monitor and target people? Will they act responsibly with these tools?"

Raji says the decisions on how to use the tech must be discussed and regulated, especially since it was found to have been used by the Hong Kong government to track and identify protestors. "Even if they did build it to find missing children, they now have that power and could easily re-orientate it. There are no safeguards in place to assure a certain amount of community input, or elective or democratic decision-making, before they use the tech for each different purpose," she says.

Insider or outsider: the ransomware conundrum

When everybody acting maliciously on a network looks like an insider, how can companies validate and identify ransomware threats and defend themselves appropriately?

Security operations teams in large organisations around the world are struggling to defend their networks against ransomware, either from targeted human-operated attacks or highly automated opportunistic campaigns. Such threats will specifically target particular companies by spear-phishing key people or actively scanning their networks for vulnerabilities. Others adopt a spray-and-pray approach, such as sending malicious resumes to human resources teams or mass scanning the whole internet when new vulnerabilities are disclosed and actionable.

The global ransomware supply chain is becoming increasingly advanced and optimised for attackers. In some cases, different people will conduct the phishing attacks or exploit vulnerabilities to gain access, selling it to cybercriminals and fraudsters who wish to ransom businesses or steal their data. Once adversaries are inside a network, they escalate privileges and move to their target just like an insider threat. They use the same tools and commands as a disenfranchised system administrator might to encrypt the entire company network or exfil data.

The only difference is, at early stages, they're not yet authenticated and they don't have legitimate credentials. Therefore, attackers immediately seek to escalate privileges and move laterally to things that matter. In ransomware attacks, they race to an administrative level of credentialing which allows them to very quickly broadcast malicious software to lock up key portions or even all a corporate network. Understanding how privilege escalation and lateral movement works is crucial because such techniques allow ransomware groups to get administrative rights and behavioural analysis solutions can't detect many of the key approaches.

"The goal of an external attacker is to become authenticated traffic on a network. Once they do that, it's very difficult to differentiate them from legitimate authenticated traffic," says Jason Crabtree, co-founder and chief executive of technology company QOMPLX.

"Authentication is fundamental to understanding who is doing what on a network, and whether or not actions and activities are being taken by the appropriate people. But simple perimeter hygiene and edge-hardening activities will not prevent ransomware attacks. Though important, multi-factor authentication is also insufficient on its own because of the plentiful ways of bypassing it, especially within enterprises that have directory services and single sign-on enabled, which is practically all of them."

QOMPLX looks at all of the details that are associated with who did what to whom in the network, recording and validating every single log-on or authentication event. "We do that with a finer grain comb than any other provider," says Crabtree, "We don't just have the metadata, but we also analyse and validate things like the Kerberos protocol with stateful streaming analytics."

The company then combines all of that data from active directory and authentication with other data feeds from existing security appliances to allow organisations to contextualise the information and achieve a greater understanding of the malicious activity in their IT. Due to the growing frequency and severity of ransomware attacks, QOMPLX has also built an elite special situations advisory services group for helping large organisations respond to ransomware threats, while simultaneously aiding in containment, eradication, restoration and sustainable uplift of security programmes.

"QOMPLX's special situations advisory group is really focused on helping companies get well and stay well, as opposed to incident response or simply getting an audit, assessment or pen test," says Crabtree. "Those do not get to the core issues with sustainable programmes and practices supported by very advanced technology that provides deep amounts of visibility and a single source of truth.

"That truth has to be continually updated and remain ground truth, rather than outdated risk registers, which are often very optimistic views of the health and state of a network or security programme. Organisations can then look at contextual challenges to re-authenticate, including with active measures triggered by our platform, like biometric multi-factor re-authentication requests, but doing that before the basics is foolish because it's easily bypassed if the fundamentals aren't right."

> **The goal of an external attacker is to become authenticated traffic on a network**

2020 DATA BREACH INVESTIGATIONS REPORT, VERIZON

4k
the number of breaches documented by Verizon

157k
the number of cyber incidents analysed by Verizon

922k
median number of login attempts encountered by firms in credential stuffing attacks

80%
of breaches involved the use of lost or stolen credentials or brute force attacks on credentials

2020 Verizon DBIR

For more information please visit qomplx.com

QOMPLX:

PAYMENTS

Invoice emails are the new Trojan horse

They are an everyday part of business, but invoice emails are the latest vehicle for tricky fraudsters and are getting increasingly hard to detect

Nick Easen

Receiving an email request from a co-worker to pay an invoice happens every minute, of every hour, of every day. So do fraudulent ones. Online criminals are increasingly targeting those who hold the corporate purse strings. Working from home during the pandemic, the finance department has been rich pickings for so-called business email compromise, or BEC, a type of fraud that costs billions.

The surge in targeted chief executive or chief financial officer fraud, as it's also known, has seen cybercriminals exploit the lockdown with coronavirus-themed campaigns that trick unsuspecting employees. According to Abnormal Security, during May there was a 200 per cent spike in the United States, where it accounts for half of all cybercrime-related financial losses. The FBI *Internet Crime Report* puts the cost at $1.77 billion a year. The UK is not immune and is second in the world after America in terms of the number of attacks.

"Many criminals are exploiting the fear and confusion stirred up by COVID-19. We've seen them impersonating senior members of company staff who then intimidate employees into making urgent payments. We've also observed con artists contacting businesses claiming to be government officers administering special coronavirus-related tax grants," says Amanda Finch, chief executive of the Chartered Institute of Information Security.

As digital cyber-defences get more sophisticated, BEC continues to slip under the radar. That's because the perpetrators don't need to be expert programmers or whizzy malware authors; they don't need to be elite hackers or past masters in network intrusions.

"What they do have is patience, persistence and advanced-level skills in social engineering. In old-school terminology, you'd call them confidence tricksters," says Paul Ducklin, principal security researcher at Sophos.

"The idea behind this crime is simple: get hold of the email password of someone important in finance, read their email before they do, learn how they operate, find out what the company is up to and when big payments are coming up then misdirect employees, creditors and debtors. Once the operation is up and running, they aim to keep the misdirection going for as long as possible by mixing social engineering skills with insider knowledge."

Uncertainty among staff is a key weapon for this type of scammer; leveraging trust is their preferred method, as well as using spoofed compromised accounts, stolen credentials and malware to get inside email accounts. BEC attackers don't need to crack passwords themselves to gain entry into servers either, they can buy them from other criminals on the dark web.

> **What cybercriminals do have is patience, persistence and advanced-level skills in social engineering**

Insurance claims received by Aviva highlight the seriousness and increasing complexity of BEC attacks. "One corporation was alerted to a bank transfer following an engineered call from their CEO, which was generated using machine-learning to recreate the call using the CEO's voice," says Patrick Tiernan, Aviva's managing director of UK commercial lines.

Deepfake technology is the latest frontier for this type of fraud. Images, voice and video can all now be replicated accurately. With so many people working remotely as a result of the pandemic it means employees are less able to verify legitimate requests. Combine this with scams that cite the impact and urgency of the health crisis and you have a perfect cybercrime storm.

"Many criminals who breach as a side job were forced to work from home or their shifts were curtailed throughout lockdown, leaving them with more time and motivation to make up their income elsewhere," says Matt Aldridge, principal solutions architect at Webroot. "This is a toxic cocktail for increased attacks."

Since most attacks follow a simple pattern, employees can be trained to spot less sophisticated ones, although some training programmes were stopped during lockdown. Simulated phishing exercises help, as does multi-factor authentication and DMARC, an email authentication protocol.

"Enforced re-logins from different network environments and regular password changes can make a difference," says Fiona Boyd, head of cybersecurity at Fujitsu. "But all the training in the world cannot help employees to spot something suspicious if an instruction is received from a senior executive's email address."

The biggest defence against business email compromise is therefore behaviour-centric cybersecurity solutions. Technology is now better at spotting people's actions that aren't quite right. "It's only when users begin acting out of character or in ways contrary to policies that businesses will begin to spot threats in their early stages," explains Audra Simons, director of Forcepoint Innovation Labs.

Technologies such as machine-learning can now help detect unusual behaviour, relationships or content that pops into employees' email boxes. Data science then decides whether an email is an attack or not. It is a new line of defence against BEC fraud.

"Some solutions model the behaviour of cybercriminals with threat intelligence to detect email attacks. We model the behaviour of individuals and organisations, and then determine whether an email is an attack, if it falls outside a particular baseline of activity," says Kenneth Liao, vice president of cybersecurity strategy at Abnormal Security.

"We have to remember that these attacks leverage social engineering tactics and do not use malicious attachments or links. This approach slips by all traditional security controls that look for threat indicators, which don't actually exist with

these attacks. So many organisations have given up on addressing this problem and point to security awareness training as the solution. This is unfortunate because there is now new technology that can address these attacks."

Aside from people and tech, there's a third line of defence: processes. These can go a long way to combating this type of fraud. Those companies that rigorously get everything countersigned, with strict controls in place, with second or third opinions needed before payment are at an advantage.

"It is worth revising your accounts payable and receivable to include cross-checks at every stage where payments and account changes are involved. If in doubt, don't give it out," says Ducklin at Sophos. Certainly, there is no single approach that will guarantee protection against BEC, but at least there are now a lot more tools.

Synthetic identities the next frontier in privacy fraud

Synthetic identity fraud occurs when criminals combine real and false information into new, bogus identities. It's used to apply for credit, loans or buying goods. While banks and other financial services haven't been accessible for many in person during lockdown, which means they can't verify peoples' ID, this type of fraud has come into its own online.

"In the United States it's the fastest growing type of financial crime. There's no reason this won't soon be true in the UK and Europe, if it's not already," says Joe Bloemendaal, head of strategy at Mitek. "Since these patchwork identities look legitimate and fraudsters are trained to mimic normal behaviour, anti-fraud measures might not recognise the threat."

Most synthetic identities go unnoticed, yet they're hidden time bombs. Fraudsters slowly build up excellent credit or show legitimate transactions on marketplaces only to bust out and leave huge unpaid debts. Machine-learning can identify this fraud, but the issue is training it on a large enough dataset of real identities to spot the fake ones. Biometrics with selfies and multiple forms of ID are being used to combat it.

"The nefarious possibilities of synthetic identities are huge. They could even play a part in large-scale money laundering schemes," adds Bloemendaal.

Solving the global identity crisis

Identity has become hugely fragmented, but the cause is also the cure

Identity itself has become fragmented due to the proliferation of online accounts. Already widespread, data breaches have further accelerated in the wake of the coronavirus pandemic, with fraudsters preying on people spending longer in digital environments and companies relaxing policies and policing to accommodate remote working. The door has opened for them to prey on the desperate and even caused some of the desperate to commit fraud themselves.

Organisations can take their pick among big data companies that supply traditional data such as credit card information, credit history and government information. Yet while these were previously data sources they could rely on to inform decisions or make risk more transparent, the growing prevalence and sophistication of cybercrime has exposed them to compromise. Traditional identity elements are, therefore, increasingly insufficient on their own for identity verification and far too thin for use in investigations.

"Identity attributes have become more numerous and scattered across the digital landscape," says Robert Nendza, vice president of corporate communications at Pipl, an information services company with the world's largest people search engine. "People actually have many identities on the internet in the form of online accounts and publicly accessible records. Individually these are weak identity elements, but together they form a strong corroborated identity.

33%

rise in financial product fraud between March and April

Experian 2020

273%

annual increase in the number of records exposed to a data breach in the first quarter

RiskBased Security 2020

65%

projected increase in FBI IC3 fraud reports

Frankonfraud 2020

"On the other hand, if you're going to use a credit card number and email address to validate someone is who they say they are, but that information is sold on the dark net, what good is that? It's a major problem. All of this supposedly secure and protected data is practically public information if you have access to the dark web. Each piece of data also only has a single source. The only place to corroborate a credit card number, for example, is with the card issuer."

Ironically, the cause is also the cure: the internet. Online identities that are collected and corroborated from many disparate sources are inherently richer. By utilising numerous sources, some proprietary and some public, online identities provide a trustworthy dataset that reduces case resolution time and makes risk far more transparent. This creates strength and trustworthiness in the online identity and it's very difficult to spoof.

As the world's leading provider of online identity information, Pipl solves the identity crisis while also bringing order to the chaos created by the COVID-19 pandemic. Pipl's proprietary identity resolution technology connects publicly available online and offline information from millions of sources. Businesses can search with a variety of parameters to find everything about a person, including personal, professional, demographic and contact information.

With Pipl, organisations can turn a single datapoint into a trusted identity to accelerate investigations and fight fraud. The key elements of an online identity solution are global data, email addresses, social connections and mobile phone numbers. Traditional sources don't have the latter, but Pipl does and has been collecting and connecting this data for more than 12 years. With unmatched coverage of more than three billion online identities, it makes connections to locations, companies, schools, friends, relatives and social media accounts.

"Pipl is the magnet that brings all data attributes together into a form where they become valuable for professional identity verification and investigation," says Nendza. "Our identity resolution engine has a recursive algorithm. When you enter a piece of data, it will continuously match and corroborate until it has many sources and a highly corroborated identity profile. That's enormously valuable not just for rapid transaction approvals, but also for investigators, who although not trying to make a decision quickly, are trying to uncover connections and reduce case resolution time.

"Investigators want to be able to uncover things they wouldn't have been able to find otherwise. Pipl builds a much more complete picture of a person's true identity, making it more difficult for fraudsters to use faked or stolen identity elements, and much easier for fraud detection systems and fraud professionals to accurately process cases and transactions," Nendza concludes.

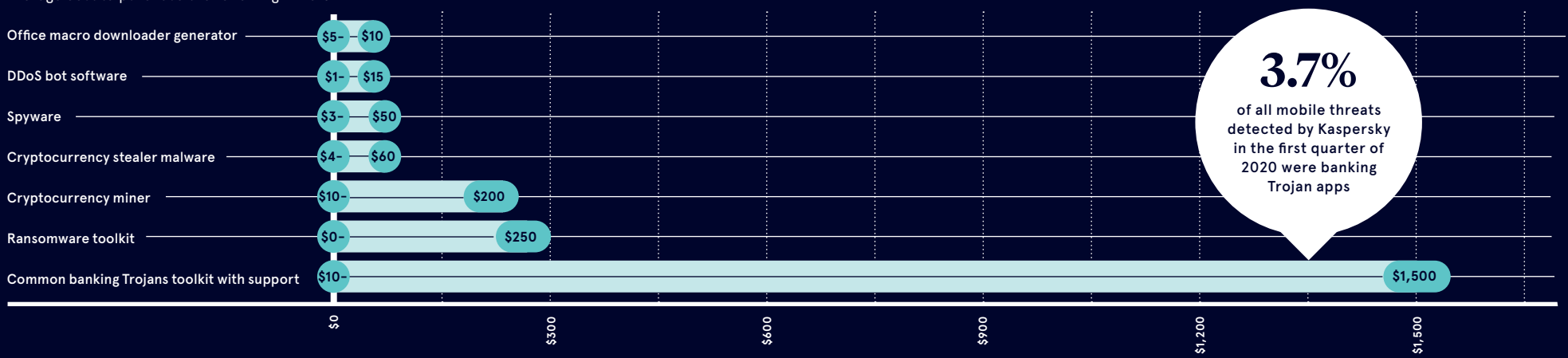
THE DARK WE

The Dark Web is used for a whole host of nefarious and illicit activity, especially when it comes to purchasing stolen data or procuring the services of professional hackers. Analysis from Trend Micro shows that $1.5 trillion is generated from cybercrime services offered on Dark Web marketplaces each year, and according to Symantec, details of just ten credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cybercriminals each month. So it's easy to see how this has become a lucrative market for so many.

BUYING MALWARE ON THE DARK WEB

Symantec/Broadcom 2019

Average cost to purchase the following in 2019



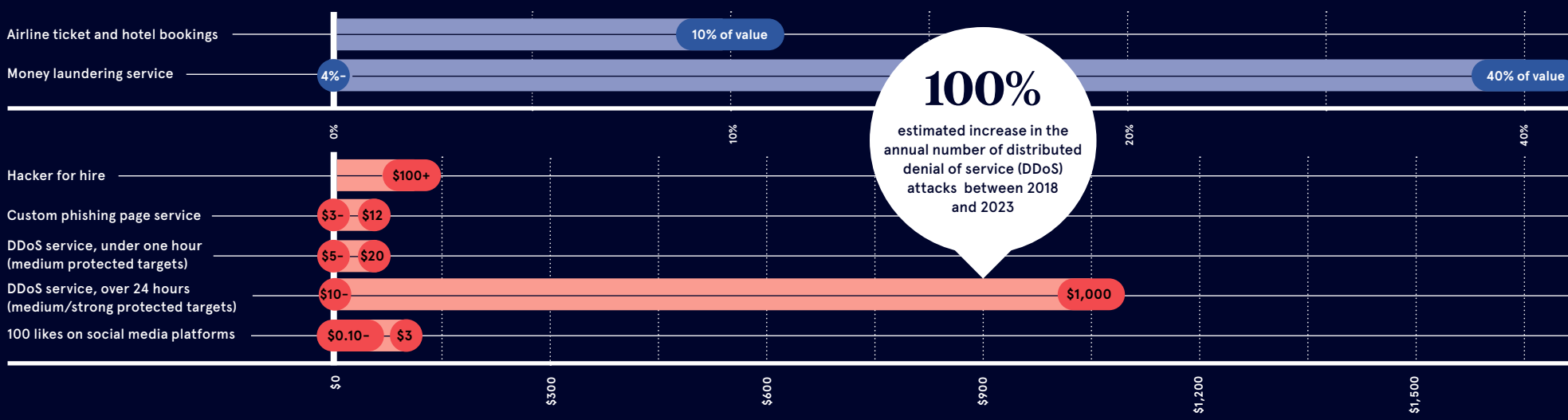
3.7%

of all mobile threats detected by Kaspersky in the first quarter of 2020 were banking Trojan apps

BUYING SERVICES ON THE DARK WEB

Symantec/Broadcom 2019

Average cost to purchase the following in 2019

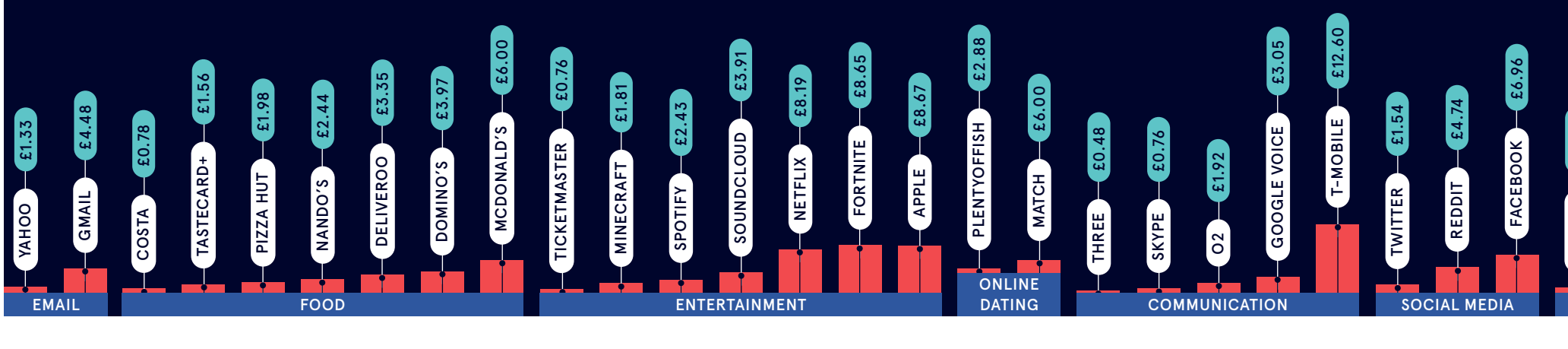


100%

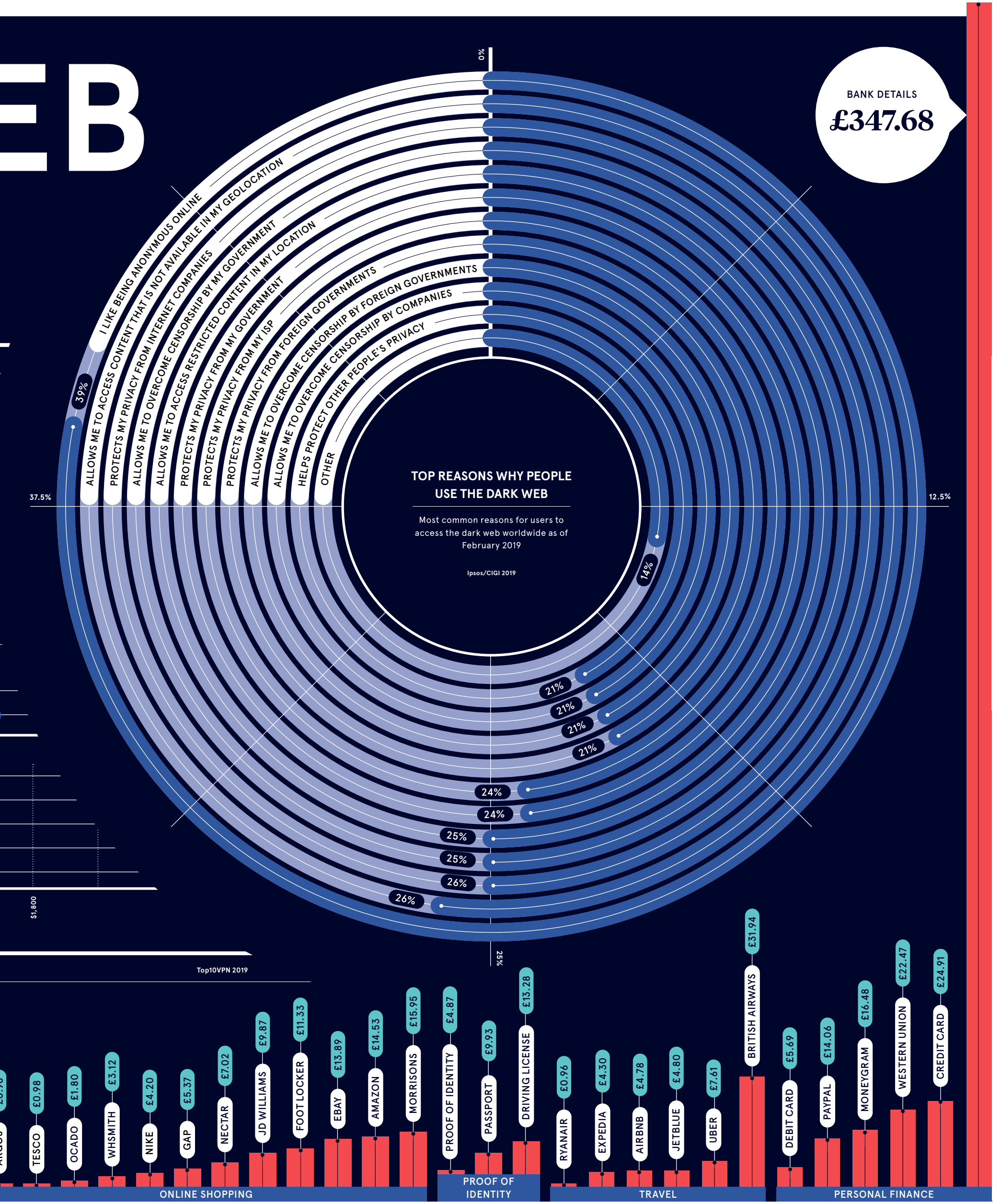
estimated increase in the annual number of distributed denial of service (DDoS) attacks between 2018 and 2023

COST OF STOLEN CREDENTIALS ON THE DARK WEB

Analysis of digital items (stolen ID, personal data and hacked accounts) for sale on the three largest active dark web markets; prices as of February 2019



EB


BANK DETAILS
£347.68
TOP REASONS WHY PEOPLE USE THE DARK WEB
Most common reasons for users to access the dark web worldwide as of February 2019
Ipsos/CIGI 2019
0%
I LIKE BEING ANONYMOUS ONLINE
ALLOWS ME TO ACCESS CONTENT THAT IS NOT AVAILABLE IN MY GEOLOCATION
PROTECTS MY PRIVACY FROM INTERNET COMPANIES
ALLOWS ME TO OVERCOME CENSORSHIP BY MY GOVERNMENT
ALLOWS ME TO ACCESS RESTRICTED CONTENT IN MY LOCATION
PROTECTS MY PRIVACY FROM MY GOVERNMENT
PROTECTS MY PRIVACY FROM MY ISP
ALLOWS ME TO OVERCOME CENSORSHIP BY FOREIGN GOVERNMENTS
ALLOWS ME TO OVERCOME CENSORSHIP BY FOREIGN GOVERNMENTS
HELPS PROTECT OTHER PEOPLE'S PRIVACY
OTHER
39%
37.5%
12.5%
14%
21%
21%
21%
21%
24%
24%
25%
25%
26%
26%
25%
$1,800
Top10VPN 2019
TESCO £0.98
OCADO £1.80
WHSMITH £3.12
NIKE £4.20
GAP £5.37
NECTAR £7.02
JD WILLIAMS £9.87
FOOT LOCKER £11.33
EBAY £13.89
AMAZON £14.53
MORRISONS £15.95
PROOF OF IDENTITY £4.87
PASSPORT £9.93
DRIVING LICENSE £13.28
RYANAIR £0.96
EXPEDIA £4.30
AIRBNB £4.78
JETBLUE £4.80
UBER £7.61
BRITISH AIRWAYS £31.94
DEBIT CARD £5.69
PAYPAL £14.06
MONEYGRAM £16.48
WESTERN UNION £22.47
CREDIT CARD £24.91
ONLINE SHOPPING
PROOF OF IDENTITY
TRAVEL
PERSONAL FINANCE

Russell Hart / Alamy Stock Photo

CRIME

A sheep in wolf's clothing

Questioning the Serious Fraud Office over its financial crime-busting credentials

Richard Brown

A watchdog with no canines makes a toothless guardian. When that sentinel is taxpayer-funded to protect against, capture and prosecute serious fraudsters, people expect its bite to be far worse than its bark.

Yet over the past few years, the UK's Serious Fraud Office (SFO) has had to endure a reputational onslaught from a litany of collapsed cases, acquittals after trial, botched investigations and the contentious use of deferred prosecution agreements (DPAs).

So bruising has the battery of failures been that merging the SFO with the National Crime Agency has been seriously considered to create a UK version of the United States' Federal Bureau of Investigation.

There was the embarrassing fiasco of three Barclays' executives being tried twice over the bank's bailout by Qatar in 2008. After an estimated £10 million of public funds spent over a seven-year investigation, a jury this February took just five hours to acquit the three bankers of lying to the market about Qatari investors' secret £322-million side deals.

Blunders in case preparation for the 2014 prosecution of three former Tesco chiefs over a missing £250 million in the supermarket's accounts led the trial judge, Sir John Royce, to lambast the SFO's case as "so weak that it should not be left for a jury's consideration".

And only last month, the SFO prematurely dropped a bribery and corruption case against banknote printer De La Rue relating to a deal to print cash for South Sudan. The fraud-busting agency has even faced accusations of a toxic corporate culture bedevilled by internal bullying and favouritism.

Marking her second anniversary next month as SFO director, Lisa Osofsky was recused from the Barclays case, while the Tesco defendants were charged before she took the helm. She is, however, sanguine about the agency's past failures, while optimistic over future opportunities.

"We take on the most serious and complex economic crimes, and each case can have unprecedented challenges and involve complicated legal issues. We hold wash-ups when we complete cases and work hard to ensure we learn any relevant lessons to improve subsequent performance. We share this knowledge across the office," she says.

"Ultimately, however, each case turns on its own facts and depends entirely on its own specific circumstances. We will always seek convictions in cases where we meet the code test for crown prosecutors and find that the evidence points to wrongdoing. Not every case is going to result in a conviction; that is not the jury system. If it did, I would not be taking on the right cases."

The code test sets out the general principles which crown prosecutors should follow when they make decisions on cases, including weighing up whether there is enough evidence against a defendant.

Below right: SFO director Lisa Osofsky

> **There is a mischaracterisation of DPAs as a 'get-out-of-jail-free card' for corporate offenders, but they do not let anyone off the hook**

A former FBI deputy general counsel, who also reported on money laundering at Goldman Sachs International, Osofsky robustly defends the use of DPAs.

First introduced in the UK in 2014 via the Crime and Courts Act 2013, these voluntary deals stave off criminal prosecution in exchange, typically, for a financial penalty and a commitment by a company to behave ethically and within the law.

The SFO celebrates the largest ever corruption-related DPA in the world, involving global aerospace firm Airbus, which the agency entered into in conjunction with French and US authorities in January. Under the terms of the DPA, Airbus agreed to a fine and costs of €991 million in the UK, from a total levy of €3.6 billion for bribery.

The DPA reached with Tesco included a fine of £129 million, while that concerning Rolls-Royce, after a four-year bribery and corruption probe, amounted to £407 million. In February 2019, the SFO dropped its investigation against unnamed individuals linked to the Rolls-Royce case following "a detailed review of the available evidence and an assessment of the public interest".

Rahul Rose, a former senior investigative officer at Corruption Watch in London, slammed the Rolls-Royce DPA as creating 'the perception that British blue-chip companies can engage in the most egregious corruption, but still escape prosecution by paying substantial sums of money to the government".

Osofsky refutes this contention. "There is a mischaracterisation of DPAs as a 'get-out-of-jail-free card' for corporate offenders, but they do not let anyone off the hook. You can't send a company to jail and a criminal conviction for a corporate creates collateral damage to employees, customers, suppliers and shareholders," she says.

"This may be appropriate for some companies, which appear unchanged and unrepentant for wrongdoing. In such cases, we would pursue prosecution. But if a company accepts responsibility for wrongdoing, demonstrates contrition and a desire to make amends and gets its house in order, the public interest favours punishing the company, while giving it the chance to demonstrate it has changed for the better."

95%

of all the evidence the Serious Fraud Office reviews is now digital

The SFO chief is adamant this is exactly what DPAs do, by providing punishment in the form of fines and disgorgement with terms that tie the corporate to compliance procedures, which will prevent future wrongdoing.

"If the terms are not met, we can resume a prosecution. We always consider prosecuting individuals in connection with corporate resolutions. But even where we do, a criminal conviction is never certain. Nor should it be; a core tenet of our justice system is a defendant's right to a fair trial," she says.

Osofsky concedes as uncomfortable last July's report by Kevin McGinty, chief inspector of the Crown Prosecution Service, into perceived favouritism and allegations of bullying within the SFO. Yet she argues that the culture, which has developed over the SFO's 30-year history, will benefit from the organisation's culture change programme, designed to stamp out negative behaviours.

Looking to the future, Osofsky points to expanded use of machine-learning tools to identify material covered by legal professional privilege and to uncover patterns and target searches of evidence. Last year, the SFO reviewed 37 million documents; 95 per cent of its evidence is now digital. Overall, a transformative new broom sweeping through the corridors of the SFO seems to have arrived none too soon. Whether the various changes Osofsky has implemented go far enough, only an uptick in fraud conviction rates will truly assuage the agency's manifold critics.

Serious Fraud Office

Commercial feature

Mobile is the new battleground for fraudsters

As fraudsters find ways to exploit superapps, digital wallets and ecommerce platforms, businesses must adopt a new approach to fraud detection that is powered by artificial intelligence and encompasses the entire user journey

While the first wave of digital fraud was caused by the migration of physical credit cards to digital payments, a second wave is now seeing fraud move to mobile applications.

By offering multiple products and services on a single platform, superapps and digital wallets risk complicating fraud risk management. In addition to payments, companies now have to deal with diverse types of fraud, such as account takeovers, fake registrations, promotional code exploitation, loyalty fraud and other reward-based loopholes.

Cybercrime was traditionally the domain of professional hackers who break into enterprises and governments to steal funds or personal data, or to cause reputational harm. But the arrival of a more digital-native generation has democratised their techniques, enabling opportunists to exploit online platforms, such as mobile apps, given their immense popularity.

Blinded by perceptions that mobile environments are more secure and being unaware of the malicious tools available to fraudsters, many businesses are unprepared. Such tools can change device profiles, manipulate physical or internet addresses, clone apps and even tamper with them.

Consumers are readily granting access to their smartphone data to enjoy a more personalised user experience, but by doing so they often become collateral damage in the ongoing hunt by fraudsters for financial gain.

"We have seen companies suffer tens of millions of dollars in fraud losses in a matter of days," says Justin Lie, founder and chief executive of SHIELD, a global cyberfraud protection company that leverages over a decade of domain intelligence and artificial intelligence (AI) to help enterprises prevent fraud in real time.

"This can be business-ending for smaller startups or fledgling companies. 7-Eleven in Japan lost half a million dollars and shut down its new app offering mobile payments within a month of launch.

"The more unsecured and profitable mobile landscape has drawn fraudsters who traditionally target ecommerce platforms. There is a new war being waged and the battleground is your smartphone. As a new attack vector ground, mobile apps require a different class of fraud detection and prevention solutions and tactics."

New weapons and attack vectors

Sophisticated fraud syndicates employ customised tools to mimic the behaviour of real users. Tampered apps, in particular, open many new possibilities for them. The more services an app offers, the more opportunities there are to exploit.

When fraudsters constantly change their attack patterns, traditional static defence mechanisms are ineffective. Solutions need to be precise, targeted and adaptable to minimise false positives while blocking fraud accurately. Otherwise, businesses risk significantly hindering their customers' user experience and suffering revenue losses.

At the same time, growing competition to establish market dominance in the digital age has driven the rise of online promotions and reward offers designed to lure consumers with attractive discounts. Popularised by the likes of WeChat and Alipay, these discounts are common on superapps such as Grab and Careem, while ride-hailing companies like Uber give out free rides to attract customers.

Fraud on these kinds of platforms can be cheap to carry out and difficult to trace. The result is a difficult operating environment for businesses relying on online and mobile-based commerce, with smartphone devices at the centre of a new battleground for fraud.

What companies must do

Companies need to urgently assess, if their fraud mitigation measures cover the threats and vulnerabilities that they face.

The first question they need to ask themselves is, do their fraud attacks only happen at the point of payment? Fraud commonly happens across the entire user journey. Promotion codes attract not only new users but fraudsters too.

> **There is a new war being waged. Mobile apps require a different class of fraud detection and prevention solutions and tactics**

Secondly, do companies know the real extent of the fraud? Fraudsters often create multiple fake accounts, fund these accounts with illicit money and then proceed to divert these funds through a complex network before cashing them out: a classic case of money laundering, but on a new platform.

Thirdly, is the company's anti-fraud solution end-to-end, future-proof and hyper-relevant? End-to-end solutions capture and block fraud at every checkpoint, ensuring complete visibility alongside a fraud mitigation approach that can be calibrated according to the needs and risk propensity at each checkpoint.

Solutions would also do well to keep up with the latest fraud trends and tools from a global perspective, ideally through a global threat intelligence network, which helps companies block emerging fraud.

Because every business is different, a good anti-fraud solution ensures relevancy of their clients digital ecosystem by accounting for the unique circumstances and requirements.

How SHIELD can help

Founded in 2008, SHIELD was the first organisation to introduce an instant fraud prevention solution, securing the entire user journey for enterprises. Its AI engine crunches millions of datapoints, performing real-time pattern recognition to identify fraud. SHIELD's self-learning algorithms constantly adapt to deliver risk assessments for each user activity in less than 70 milliseconds, ensuring its clients' customers can continue to transact without affecting user experience.

SHIELD profiles more than seven billion devices and 500 million user accounts globally. The plug-and-play nature of its solutions helps simplify fraud management and secure digital ecosystems from end to end through a single application programming interface, or API. Fraud attacks against their clients are uploaded in real time to its global intelligence network, enabling other clients around the world to block similar attacks.

7bn

devices profiled by SHIELD worldwide, along with 500 million user accounts

<70ms

for SHIELD's self-learning algorithms to deliver risk assessments for each user activity. This ensures a seamless user experience for clients' customers to continue transacting

"The future of cyberfraud is AI and it's already here," says Irene Brime, co-founder and managing director of SHIELD. "Fraudsters are using more advanced scripts and, increasingly, machine-learning to fine-tune and vary their attacks. As machine-learning and AI becomes more accessible, any opportunist has the potential to be a fraudster.

"SHIELD's mission is to be the only autonomous risk intelligence solution that enterprises need to scale without risk. With end-to-end protection of the user journey, enterprises are kept safe from fraud while ensuring their products and services reach the largest number of real users, maximising their profit margins. We help clients achieve a better and safer customer experience, making the internet a safer place for everyone."

For more information please visit shield.com

SHIELD
Autonomous Risk Intelligence

RANSOMWARE

Giving in to the hackers

Paying to get stolen data back following a ransomware attack often seems the only course of action, but you may pay double in the long run

JMiks/Shutterstock

Emma Woollacott

In early June, Michigan State University revealed it had been hit by hackers using Netwalker ransomware; at the same time, the University of California, San Francisco experienced a similar attack.

In both cases, the hackers encrypted data held on university servers and demanded a ransom for its release, but the two institutions responded in very different ways.

Both were able to lock down quickly, limiting the amount of data that was compromised, and both reported the breach to users and law enforcement. But while MSU refused to hand over the ransom, UCSF paid up.

"The data that was encrypted is important to some of the academic work we pursue as a university serving the public good," the UCSF explained in a statement.

"We, therefore, made the difficult decision to pay some portion of the ransom, approximately $1.14 million, to the individuals behind the malware attack in exchange for a tool to unlock the encrypted data and the return of the data they obtained."

Ransomware attacks such as these have been on the rise for some time and the growth has only accelerated during the coronavirus crisis. In March, according to security form VMware Carbon Black, ransomware attacks shot up 148 per cent from February.

And there's also a trend towards paying up, with a recent survey carried out for insurer Hiscox finding one in six organisations experiencing a ransomware attack in the last year has handed over the cash.

Traditional wisdom is this is a bad idea. Law enforcement agencies don't like it as it encourages the criminals.

But Josh Zelonis, principal analyst with Forrester, says it may make sense to consider paying the attackers, much as it may stick in the craw. This means taking a careful look at precisely which systems have been impacted.

"I know of one particular situation where they didn't pay the ransom because of the systems that were hit; they were critical, but not so critical," he says.

"The comment that was made to me was that if they'd encrypted these other systems, they'd have paid instantly."

Many organisations are unprepared for an attack, making it more likely that they'll be forced to pay up. Indeed, says Zelonis, even where organisations do regularly backup their data, most fail to check their backups.

"In a survey I did, the vast majority of companies, which tested their ability to recover from an attack, backup once a year and something like 90 per cent of backups complete with errors, and the severity of these errors is to be determined," he says.

"So a lot of organisations are running these costly backup solutions and don't actually know whether those backups are going to work until somebody's gone and encrypted their infrastructure."

However, paying up certainly isn't a way of magically making the problem go away. According to John Shier, senior security expert at Sophos, the average cost of a ransomware attack where the ransom is paid is $1.4 million, almost twice as much as where the ransom is denied.

"When you get hit by ransomware, it's because there's some sort of deficiency in your protection," he says.

"So the act of paying the ransom only solves part of the problem – the problem of getting your encryption keys and the restoring of your files – but it doesn't resolve the underlying problem, which is whatever the criminals exploited in the first place to get on to your network. That hole still exists."

It's also worth remembering that paying the ransom doesn't necessarily mean things will get back to normal. A Sophos study found that just 26 per cent of ransomware victims whose data was encrypted got it back by paying the ransom, though results differed drastically by geography, from 66 per cent among Indian organisations to just 4 per cent in Italy.

> **A lot of organisations are running costly backup solutions and don't actually know whether they are going to work**

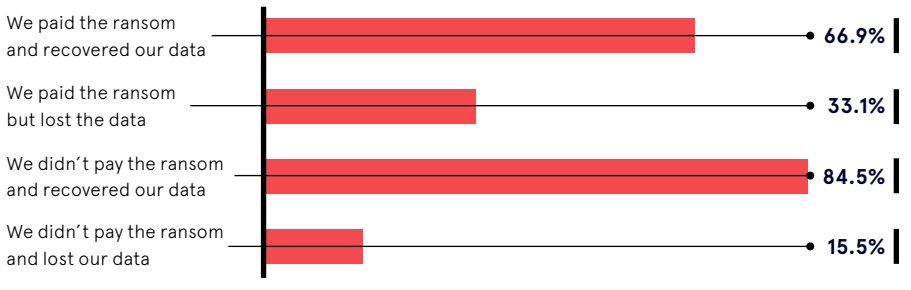
To an extent, it's possible to plan whether a ransom should be paid, and the important thing is to ensure the organisation is in a position to make a quick decision.

"You can prepare ahead of time. You can get your business stakeholders together and put together a plan for if the worst happens," says Shier.

"When something unforeseen forces your hand, that's when you make a last-minute decision, but you have to have all your stakeholders in place."

TO PAY OR NOT TO PAY CyberEdge 2020

According to global IT decision makers, the following actions were taken after their organisations were victimised by ransomware in the 12 months to November 2019



OPINION

‘It’s not a question of if we see more fraud, it’s a question of how much and how prepared we will be”

The coronavirus pandemic is unprecedented in many ways and we are already seeing its impact. As the president and chief executive of the Association of Certified Fraud Examiners (ACFE), the world's largest anti-fraud organisation, I know that during times of chaos and uncertainty, fraud increases so organisations need to brace themselves.

Two of the biggest challenges organisations will face in the wake of the pandemic are an increase in attempted fraud, from both insiders and outside parties, and mounting hurdles that prevent anti-fraud professionals from doing their job to the greatest effect.

There are many reasons fraud proliferates during times of economic instability. One factor is the increased pressure companies and their employees feel as they struggle to meet the challenges of a down economy. For example, struggling companies can face pressure to falsify their financials to meet earnings targets or secure financing.

Economic pressure also affects a company’s employees and can make the company a target. In times of economic crisis, employees might face salary reductions, potential furloughs or loss of a partner’s income.

When employees’ personal financial pressures rise, they may be more likely to steal from their employers. The ACFE’s 2020 Report to the Nations shows 42 per cent of occupational fraudsters are living beyond their means and 26 per cent are experiencing financial difficulties at the time they commit fraud.

Outside fraudsters also see instability as opportunity. According to data in the ACFE’s Fraud in the Wake of COVID-19: Benchmarking Report, 81 per cent of anti-fraud professionals surveyed in May 2020 have already seen an increase in cyber-fraud, such as business email compromise, hacking and ransomware, with 45 per cent saying this increase has been significant.

The COVID-19 pandemic has resulted in several circumstances that cybercriminals seek to exploit. Many employees have been working from home and their home networks may not have the same robust cybersecurity controls as their office.

Also, with operational changes and disruptions due to the pandemic, phishing attempts might not seem as out of the ordinary as they would during a normal time, leaving potential victims’ guard down.

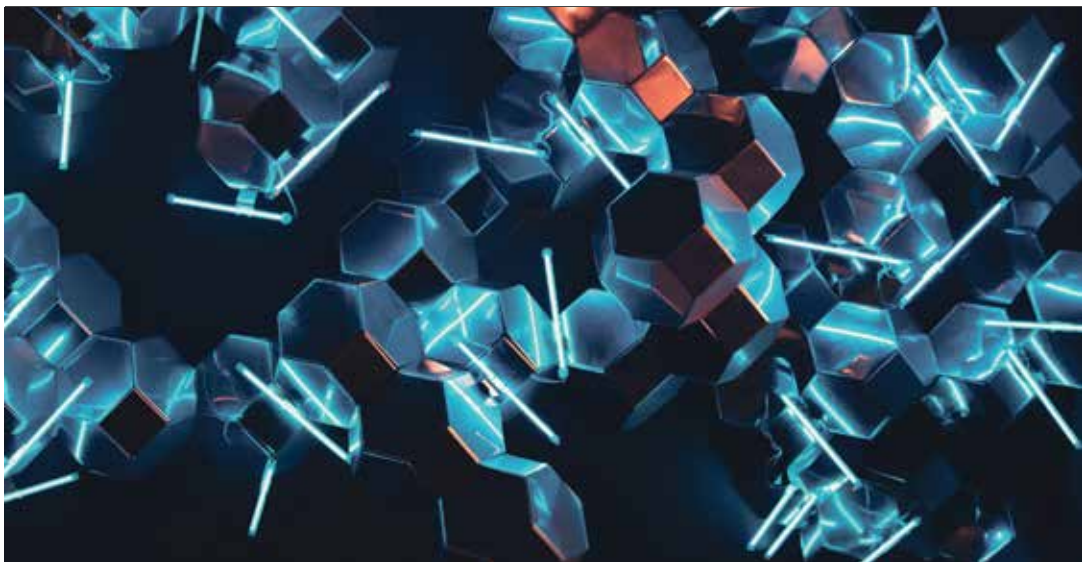
Many rules put in place by governments around the world to limit the spread of COVID-19 have affected travel and limited the ability to have in-person meetings. While these measures were necessary to halt the spread of the virus, they also present unique challenges to anti-fraud professionals.

In the COVID-19: Benchmarking Report, 74 per cent of the anti-fraud professionals surveyed said investigating fraud is more challenging in the wake of the pandemic. Specifically, the respondents cited the inability to travel (38 per cent), lack of access to evidence (32 per cent) and difficulties in conducting remote interviews (28 per cent) as some of the top challenges in combating fraud in the current environment.

At the same time, organisations that are struggling to remain profitable in unstable economic conditions may seek to cut costs and could target departments like compliance and internal audit. This is a mistake. The Report to the Nations shows organisations that fail to invest in internal controls experience significantly higher fraud losses and take longer to detect frauds than those that have anti-fraud measures in place. I can confidently say now is the time for organisations to bolster, not cut, their anti-fraud controls.

Although business practices may not be top of mind while we navigate these difficult changes, I encourage organisations to look towards the future to protect themselves, and their employees, against fraud. Because it’s not a question of if we see more fraud, it’s a question now of how much we will see and how prepared we will be to address it. ●

Bruce Dorris
President and chief executive
Association of Certified Fraud Examiners



How crime groups are adapting to COVID-19

International collaboration, sharing intelligence and expertise, can stem the rising tide of organised crime, says **Dennis Toomey**, global director, Counter Fraud Analytics and Insurance Solutions at BAE

Organised crime is a vast, sophisticated and borderless challenge. The gangs responsible are nothing if not resilient. They lie, cheat and intimidate their way to countless riches, depriving businesses, societies and governments of much-needed revenue, and profiting from human misery.

They are also incredibly agile. Amid a longer-term trend, which has seen many migrate their operations to cyberspace to preserve their anonymity, these organised crime gangs (OCGs) were among the first to react to the coronavirus pandemic.

The best way to tackle the persistent threat OCGs pose to the global economy is through collaboration. It must be cross-border, cross-industry and committed to overturning cultural resistance and institutional silos. In short, we must be as relentless in our efforts as the bad guys are.

In the shadows

Organised crime is difficult to tackle precisely because it is so nebulous. It operates in the shadows, often from behind an anonymising browser, and across geographic boundaries in Africa, Asia, the Balkans, Middle East, Eurasia, North and South America.

Larger, more traditional, OCGs may be organised hierarchically, while others may operate as part of smaller, loosely connected networks. The same networks may take on anything from trafficking drugs, people, organs and firearms to illegal mining and logging, counterfeit goods, cybercrime and much more.

> Collaboration must be cross-border and cross-industry

Accurate current data is difficult to come by, but some estimates claim organised crime is worth upwards of $2 trillion annually. That’s more than 1.4 per cent of global GDP. Europol, the European Union’s law enforcement agency, says it is investigating more than 5,000 such gangs operating internationally.

Pivoting to counterfeits

Most recently, we’ve observed just how agile these groups can be when challenged by a serious business-critical event. As an era-defining global health and financial crisis, COVID-19 has had a major impact on the kind of seamless cross-border movement of goods and people that historically allowed OCGs to flourish.

The serious disruption to global supply chains and border closures sparked by government lockdowns forced OCGs to pivot rapidly. Whereas a few months ago it may have been making money from drug and migrant smuggling across borders, an OCG is now more likely to be focused on shipping counterfeit medicines, medical products and other items currently in high demand.

Interpol’s Operation Pangea recently seized more than 48,000 suspect goods, including $14 million of potentially dangerous pharmaceuticals, in 90 countries. Some 37,000 unauthorised and counterfeit medical devices were also taken, most of which were surgical masks and self-testing kits. The international police organisation said it managed to disrupt 37 OCGs in the process, but conceded this was just the tip of the iceberg.

Beehives, not bees

Interpol is right. OCGs have the advantage of surprise. They are extremely flexible, work across jurisdictions and are unbound by local regulation or law. But the fight against organised crime is not a lost cause. In fact, the world is getting smaller, thanks to the collaborative impact of technology, which makes it easier in theory for the good guys to share vital information.

There’s no single industry or country that isn’t affected in some way by organised crime. This presents a tremendous opportunity for us to forge a truly global alliance against OCGs.

Historically this has been difficult due to organisational silos between fraud, financial crime and cybercrime teams, and a reluctance to share sensitive information for fear of the impact on corporate reputation and competitive differentiation.

But that’s changing, with initiatives like The Intelligence Network, launched by BAE Systems two years ago and now boasting more than 1,800 members. Our vision is to build a new culture through radical trust, standardise the capturing of threat information and in so doing help to make a major impact on global cyber-fraud.

We also created a global insurance fraud summit last year, bringing 16 countries and more than 50 speakers together to discuss industry best practice and how best to share intelligence. This is yet another sector that is being seriously affected by organised crime and it is ordinary policyholders that end up paying the price through higher premiums.

The bottom line is OCGs will always be with us in one form or other. But while we can’t eradicate them completely, we can greatly reduce their financial and societal impact. This means collaborating more effectively: having the confidence to share intelligence with regulators, law enforcers and industry peers so together we can achieve a common good.

This is not about swatting individual bees. It is about going after the hives themselves, to cripple these criminal enterprises at source.

For more information please visit www.baesystems.com/financialservices

BAE SYSTEMS

Commercial feature

Pandemic is a perfect storm for voice fraud

Criminals are exploiting the coronavirus pandemic to commit lucrative phone fraud, but help is at hand

With the loss of the high street in lockdown and the subsequent boom in online retail, banking and financial services, with everyone working from home, call volumes to customer service staff have spiked. The coronavirus outbreak saw businesses then scale their phone-based operations, while shifting call centre and customer-facing staff to work remotely. In the process voice fraud has soared.

Contact centre crime has already rocketed by 350 per cent in the past five years. Every year $14 billion is lost to phone fraud across the globe. Every minute of every day there are hundreds of voice channel attacks worldwide, with many consumers pointing the finger at the company they're dealing with when an attack occurs on their account. It's bad for brand reputation and the bottom line.

"Voice-based syst ems and call centres have traditionally been vulnerable to security threats and fraud. Many phone systems still are and these vulnerabilities have been exacerbated by the pandemic. Right now, there's an arms race going on with criminals using the COVID-19 crisis in highly creative ways to commit sophisticated attacks via phone," explains Mark Horne, chief marketing officer at Pindrop, a global pioneer in voice security and authentication.

"One client saw calls go up tenfold. But their capacity to cope plummeted with the closure of their call centres. Fraudsters then subjected stressed customer service staff working from home to coronavirus-themed requests that required immediate action, many to transfer money to distressed loved ones. It's created the perfect storm, especially for financial services."

Out of all those who dial in to contact centres, only 0.1 per cent are fraudulent, finding them is therefore difficult. Criminals use interactive voice response, or IVR, the self-service systems that most companies now use to verify accounts and test whether passwords work. They are able to deploy spoof telephone numbers and customer data purchased from the dark web to impersonate valid account holders.

"Sixty per cent of online fraud can be tracked back to reconnaissance work that criminals do via the IVR. Once they've breached the system, they're able to commit the attack by withdrawing funds, resetting passwords or updating contact information while on the phone to an agent or online. But there's now technology that can identify an illegitimate caller," says Horne, whose company works with Lloyds Bank Group, other top banks, insurers and etailers such as the Very Group (formally Shop Direct) in the UK.

"Education is huge part of this; consumers who use the same password for their Netflix, email and bank account are open season for attacks. Time and again we try to inform people about this. However, the battle's ongoing. It doesn't help that fraudsters now use deepfake audio to commit fraud. It is a worrying trend."

> **We can catch fraud in real time, while the criminal is on the line**

Authenticating more callers using software is now a significant trend. Artificial intelligence (AI) and machine-learning are being increasingly used to analyse calls to contact centres in a bid to counteract fraud and improve the customer experience.

"Our AI engines can process thousands of factors from an individual call, including voice, location, device type, number history, behaviour and call details. Additionally, we have one of the world's largest databases of known fraudsters. So we can catch 80 per cent of criminals even before they commit the crime," says Horne. So far, Pindrop has processed more than 1.2 billion calls and detected 1.5 million fraud attacks.

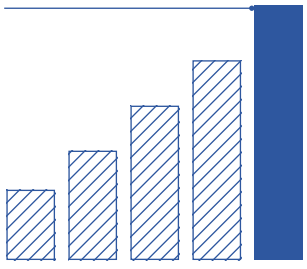
"We can catch fraud in real time, while the criminal is on the line; machine-learning algorithms operate on calls via the cloud analysing the call data. If a call centre representative looks at the risk score and it's in the red, they pass it on to a fraud team or decline the transaction immediately. At Pindrop we can now shine a spotlight on fraudulent activity in banking, insurance, etail and many more sectors before it becomes an issue. The more calls we analyse, the better we're getting at detecting fraud. It's a game-changer," Horne concludes.

Check out why voice fraud matters at pindrop.com

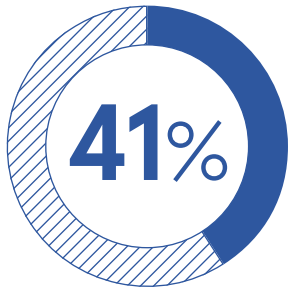
pindrop

$14bn
lost to phone fraud globally each year

350%



increase in contact centre fraud in last five years



of customers blame the brand for fraud happening

COUNTERFEITING

Protecting the real deal

Imitation may be the sincerest form of flattery, but counterfeit fashion products are costing the real deal in both reputation and revenue; new technology might be an answer

Josh Sims

These are tough times for the fashion industry and boom times for counterfeiters. Once fakes were sold on street corners. Now the underground has gone overground, with technology providing a global platform for elusive traders. A study by analytics firm Ghost Data this spring suggests that nearly 20 per cent of all posts about fashion products on Instagram, for example, feature counterfeits.

"Online has meant that access to fashion counterfeits has exploded. There are so many ways for counterfeiters to sell this stuff and the challenge is to get these channels to adopt better practices," says Bruce Foucart, deputy director of the International Chamber of Commerce's Business Action to Stop Counterfeiting and Piracy. "Are they responding? Well, yes and no."

Pressure is applied, he says, but it still typically falls back to expectations that fashion brands should be doing more to stop counterfeiters in the first place. So, if technology is providing counterfeiters with a route to market, can tech also counter counterfeiting? Holographic bubbles, radio-frequency identification chips, smart tags, blockchain – so-called check tech – are exploring every angle.

"The market for technological solutions to counterfeiting is

> **Unfortunately for fashion, copying a pharmaceutical is not easy, while copying a pair of Nikes is not so hard**

GABRIEL BOUYS/AFP via Getty Images

increasing tremendously; 20 years ago there was almost no tech being used," says Dr Fred Jordan, chief executive of anti-counterfeiting technology company AlpVision.

"The problem is that most technology being used at the moment is tech you can see: a hologram or a scannable tag, for example. Then it just becomes a battle between the users of tech and the counterfeiters finding ways around it. What's crucial now is that the tech has to be effectively invisible; counterfeiters don't respond to it because they don't know it's there. It's security by obscurity."

AlpVision's Cryptoglyph system prints an "invisible" and random digital image on packaging and labelling that only software can see. Users of the system, typically along the supply chain rather than end-consumers, assess whether a product is genuine using an app. How the app works, of course, is secret. Serious counterfeiters would need to become hackers.

But Jordan concedes that tech is unlikely to be enough; it's more a tool for brands and their lawyers to attempt to bring prosecutions. This perhaps explains why much of the work being done to beat counterfeiters is more in pursuing legislation than further tech. Nike, for example, is backing draft legislation that would give US Customs the authority to seize goods believed to infringe patented designs at the border, rather than having to go through a slow and, for small companies, prohibitively expensive trial.

Yet, what if a means of assessing the authenticity of a product could be put in the end-consumer's hands? That's the longer-term plan for Vidyuth Srinivasan, co-founder of tech company Entrupy.

Its "fingerprinting" system, which uses a proprietary optical scanner to record up to 1,200 datapoints about an object, from texture to colour contrast and even microscopic imperfections that are all unique to that object, has been trialled with a UK retail chain and is currently being used by a number of manufacturers in the handbag and accessories market. More than invisible, there's no physical record left on the object at all. Surely this is a game-changer? But he too is circumspect.

"When we started developing this technology, our idea was that we'd solve the global problem of what is, in effect, an entire shadow economy. And I think we're close to having that ultimate authentication tech," says Srinivasan.

"But still this disincentivisation of counterfeiters is mitigating what is actually a hugely complicated problem. This might allow a supply chain, retailer or eventually a consumer to guarantee the authenticity of what they buy but ,of course, it doesn't stop counterfeits being made. Tech is one part of the puzzle."

Bob Barchiesi, president of the International Anti-Counterfeiting Coalition, a non-profit co-founded by brands including Levi's, says tackling fashion counterfeiting may really be down to the huge task of changing mindset: make the purchase of fashion counterfeits socially unacceptable.

"The fact is, while it doesn't help that fashion is not a sympathetic victim [not least, it might be argued, because fast fashion has seen it rebuilt on legal copying], the money generated by counterfeiting goes on to fund organised crime, terrorism, child exploitation," he says of what's typically regarded as a low-risk, white-collar crime. "That insight resonates with consumers. The challenge for luxury goods makers is that consumers generally don't know those consequences."

Or, perhaps, consumers don't even care. Particular to counterfeited fashion goods is its desirability is in part predicated on its "exclusivity". "That means there's a lot of money to be made by people who can meet demand at a lower price point and, unfortunately for the fashion industry, copying a pharmaceutical is not easy, while copying, say, a pair of Nikes is not so hard," says Dr Amanda Budde-Sing of the US Air Force Academy's international management department and author of a paper on Australian bootmaker UGG's long trademark battle.

Tech may help keep fakes out of supply chains, which protects consumers who want to be confident they're buying the real deal. "But the fact is that, ultimately, it won't help fashion beat counterfeiting one tiny bit," Budde-Sing adds. "Because the vast majority of people, who buy counterfeit fashion, know they're buying a counterfeit and don't care."

Her new, as yet unpublished, research suggests that a counterfeit is either a stop-gap until the consumer can afford the real deal or purchased in the belief that it's as good as the real thing, but a fraction of the price. Fashion brands may be bothered by supposed lost sales, but more so by the damage to their reputation as counterfeits suggest their products are not so exclusive, after all.

"But they also have to accept the bottom line that if a high-end fashion brand isn't being counterfeited, it's because it's no longer desirable," Budde-Sing concludes.

20%

of all posts about fashion products on Instagram feature counterfeit and/or illicit products

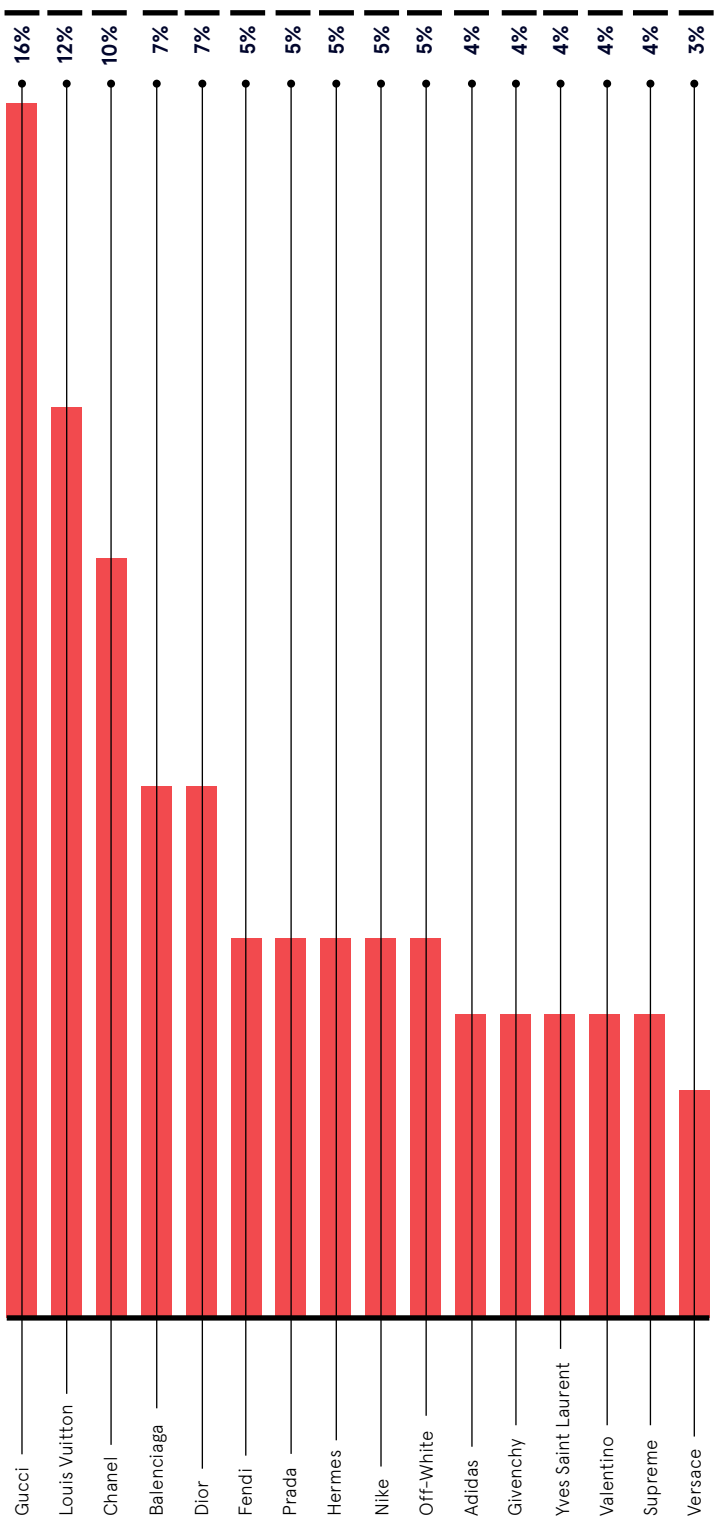
Ghost Data 2019

GABRIEL BOUYS/AFP via Getty Images

Below:
US Customs and Border Protection official examining a pair of counterfeit Christian Louboutin shoes from one of five shipments from China

TOP BRANDS MENTIONED BY COUNTERFEITERS Ghost Data 2019

Analysis of nearly 700,000 Instagram posts from counterfeiters containing the hashtags or related hashtags of the following fashion brands



IT IS A WAR OF WORDS

As cyber defences are increased, fraudsters are targeting the voice channel with sophisticated social engineering attacks aimed to execute criminal transactions, orchestrate account takeover and instigate fraudulent claims.

Has your contact centre become the weakest link in your battle against fraud?

Voice biometric anti-fraud measures alone are vulnerable to 'previously unknown' attacks.

Intelligent Voice Analytics is not - exposing fraudulent behaviour from the very first call.

With a longstanding record of success in delivering intelligence-applicable technologies and award-winning contact centre solutions, Intelligent Voice Analytics fortifies your fraud risk management programme to protect your genuine customers and defeat the fraudster.

Intelligent Voice®

lexiQal
Intelligent Voice Analytics

FIND OUT MORE, VISIT:
https://bit.ly/lexiQal-for-fraud-detection

SCAN ME