The human side of CYBERCRIME

As cyberattacks grow ever more sophisticated, those who defend against them are embracing behavioural science and economics to understand both the perpetrators and their victims.

BY M. MITCHELL WALDROP

Say what you will about cybercriminals, says Angela Sasse, "their victims rave about the customer service".

Sasse is talking about ransomware: an extortion scheme in which hackers encrypt the data on a user's computer, then demand money for the digital key to unlock them. Victims get detailed, easy-to-follow instructions for the payment process (all major credit cards accepted), and how to use the key. If they run into technical difficulties, there are 24/7 call centres.

"It's better support than they get from their own Internet service providers," says Sasse, a psychologist and computer scientist at University College London who heads the Research Institute in Science of Cyber Security. That, she adds, is today's cybersecurity challenge in a nutshell: "The attackers are so far ahead of the defenders, it worries me quite a lot."

Long gone are the days when computer hacking was the domain of thrill-seeking teenagers and college

ILLUSTRATION BY SÉBASTIEN THIBAULT

students: since the mid-2000s, cyberattacks have become dramatically more sophisticated. Today, shadowy, state-sponsored groups launch exploits such as the 2014 hack of Sony Pictures Entertainment and the 2015 theft of millions of records from the US Office of Personnel Management, allegedly sponsored by North Korea and China, respectively. 'Hacktivist' groups such as Anonymous carry out ideologically driven attacks on high-profile terrorists and celebrities. And a vast criminal underground traffics in everything from counterfeit Viagra to corporate espionage. By one estimate, cybercrime costs the global economy between US$375 billion and $575 billion each year[1].

Increasingly, researchers and security experts are realizing that they cannot meet this challenge just by building higher and stronger digital walls around everything. They have to look inside the walls, where human errors, such as choosing a weak password or clicking on a dodgy e-mail, are implicated in nearly one-quarter of all cybersecurity failures[2]. They also have to look outwards, tracing the underground economy that supports the hackers and finding weak points that are vulnerable to counterattack.

"We've had too many computer scientists looking at cybersecurity, and not enough psychologists, economists and human-factors people," says Douglas Maughan, head of cybersecurity research at the US Department of Homeland Security.

That is changing — fast. Maughan's agency and other US research funders have been increasing their spending on the human side of cybersecurity for the past five years or so. In February, as part of his fiscal-year 2017 budget request to Congress, US President Barack Obama proposed to spend more than $19 billion on federal cybersecurity funding — a 35% increase over the previous year — and included a research and development plan that, for the first time, makes human-factors research an explicit priority.

The same sort of thinking is taking root in other countries. In the United Kingdom, Sasse's institute has a multiyear, £3.8-million (US$5.5-million) grant from the UK government to study cybersecurity in businesses, governments and other organizations. Work from the social sciences is providing an unprecedented view of how cybercriminals organize their businesses — as well as better ways to help users to choose an uncrackable yet memorable password.

The fixes are not easy, says Sasse, but they're not impossible. "We've actually got good science on what does and doesn't work in changing habits," she says. "Applying those ideas to cybersecurity is the frontier."

KNOW YOUR AUDIENCE

Imagine that it is the peak of a harried work day, and a legitimate-looking e-mail lands in your inbox: the company's computer team has detected a security breach, it says, and everyone needs to run an immediate background scan for viruses on their machines. "There's a tendency to just click 'accept' without reading," says Adam Joinson, a social psychologist who studies online behaviour at the University of Bath, UK. Yet the e-mail is a fake — and that hasty, exasperated click sends malware coursing through the company network to steal passwords and other data, and to convert everyone's computers into a zombie 'botnet' that fires off more spam.

The attackers, it seems, have a much better grasp on user psychology than have the institutions meant to defend them. In the scenario above, the success of the attack relies on people's instinctive deference to authority and their lowered capacity for scepticism when they're busy and distracted. Companies, by contrast, tend to impose security rules that are disastrously out of sync with how people work. Take the ubiquitous password, by far the simplest and most common way for computer users to prove their identity[3]. One study[4], released in 2014 by Sasse and others, found that employees of the US National Institute of Standards and Technology (NIST), headquartered in Gaithersburg, Maryland, averaged 23 'authentication events' per day — including repeated logins to their own computers, which locked them out after 15 minutes of inactivity.

Such demands represent a substantial drain on employees' time and mental energy — especially for those who try to follow the standard password guidelines. These insist that people use a different password for each application; avoid writing passwords down; change them regularly; and always use a hard-to-guess mix of symbols, numbers and uppercase and lowercase letters.

CYBERCRIME COSTS THE GLOBAL ECONOMY BETWEEN $375 BILLION AND $575 BILLION EACH YEAR.

So people resort to subversion. In another systematic study of password use in the real world[5], Sasse and her colleagues documented the ways in which workers at a large multinational organization side-stepped the official security requirements without (they hoped) being totally reckless. The employees' methods — writing down a list of passwords, for example, or transferring files between computers using unencrypted flash drives — would be familiar in most offices, but essentially created a system of 'shadow security' that kept the work flowing. "Most people's goal is not to be secure, but to get the job done," says Ben Laurie, who studies security compliance at Google Research in London. "And if they have to jump through too many hoops, they will say, 'To hell with it.'"

Researchers have uncovered multiple ways to ease this impasse between workers and security managers. Lorrie Cranor directs the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University in Pittsburgh, Pennsylvania — one of several groups worldwide that are looking at ways to make password policies more human-compatible.

"We got started on this six or seven years ago, when Carnegie Mellon changed its password policy to something really complicated," says Cranor, who is currently on leave from the university to serve as chief technologist at the US Federal Trade Commission in Washington DC. The university said that it was trying to conform to standard password guidelines from NIST. But when Cranor investigated, she found that these guidelines were based on educated guesses. There were no data to base them on, because no organization wanted to reveal its users' passwords, she says. "So we said, 'This is a research challenge.'"

TOP 10 MOST COMMON PASSWORDS 2015

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball

SOURCE: SPLASHDATA (GO.NATURE.COM/BIXMEK)

Cranor and her colleagues put a wide range of password policies to the test[6] by asking 470 computer users at Carnegie Mellon to generate new passwords based on different requirements for length and special symbols. Then they tested how strong the resulting passwords actually were, how much effort was required to create them, how easy they were to remember — and how annoyed at the system the participants became.

One key finding[7] was that organizations should forget the standard advice that complex gobbledygook words such as 0s7G0*7j%x$a are safest. "It's easier for users to deal with password length than password complexity," says Cranor. An example of a secure but user-friendly password might be a concatenation of four common but randomly chosen words — something like usingwoodensuccessfuloutline. At 28 characters, it is more than twice as long as the gibberish example, but much easier to remember. As long as the system guards against people making stupid choices such as passwordpassword, says Cranor, strings of words are quite hard for attackers to guess, and provide excellent security.

CHANGING PASSWORDS EVERY 90 DAYS RANKS BETWEEN USELESS AND COUNTERPRODUCTIVE.

TIME FOR A CHANGE

Another key finding, says Cranor, is that unless there is reason to think that the organization's security has been compromised, the standard practice of forcing users to change their passwords on a 30-, 60- or 90-day schedule ranks somewhere between useless and counterproductive (see go.nature.com/2vq6r4). For one thing, she says, studies show[8] that most people respond to such demands by choosing a weaker password to begin with, so that they can remember it, and then making the smallest change that they can get away with. They might increase a final digit by one, for example, so that password2 becomes password3 and so on. "So if a hacker guesses your password once," she says, "it won't take them many tries to guess it again."

Besides, she says, one of the first that things hackers do when they break in is to install a key-logging program or some other bit of malware that allows them to steal the new password and get in whenever they want. So again, says Cranor, "changing the password doesn't help".

Sasse sees encouraging signs that such critiques are being heard. "For me, the milestone was last year when GCHQ changed its advice on passwords," she says, referring to the Government Communications Headquarters, a key UK intelligence agency. GCHQ issued a public document[9], containing several citations to the research literature, that gave up on long-established practices such as demanding regular password changes, and instead urged managers to be as considerate as possible towards the people who have to live with their policies. "Users have a whole suite of passwords to manage, not just yours," goes one bit of advice. "Only use passwords where they are really needed."

ATTACK THE ATTACKERS

If research can uncover weak points in user behaviour, perhaps it can also find vulnerabilities among the attackers.

In 2010, Stefan Savage, a computer scientist at the University of California, San Diego, and his team set up[10] a cluster of computers to act as what he calls "the most gullible consumer ever". The machines went through reams of spam e-mails collected from several major antispam companies, and clicked on every link they could find. The researchers focused on illegal pills, counterfeit watches and handbags, and pirated software — three of the product lines most frequently advertised in spam — and bought more than 100 items. Then they used specially designed web-crawling software to track back through the spammers' supply network. If an illicit vendor registered a domain name, made payments to a supplier or used a bank to accept credit-card payments, the researchers could see it. The study exposed, for the first time, the entire business structure of computer criminals — and revealed how surprisingly sophisticated it was.

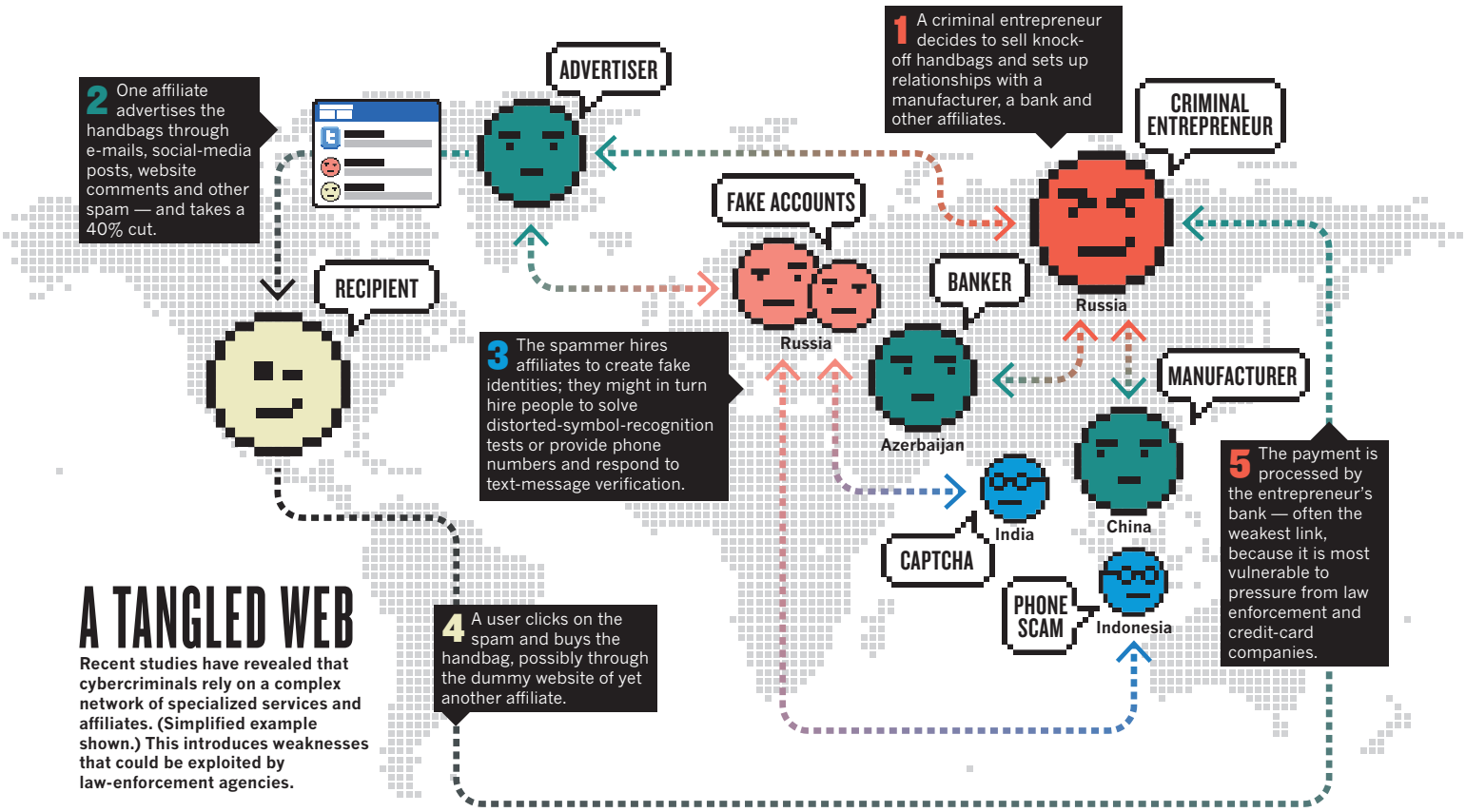
"It was the ultimate hothouse of weird new entrepreneurial ideas," says Savage, "the purest form of small-business capitalism imaginable — because there is no regulation." Yet there was order, even so. "Say you have a criminal activity you want to engage in," Savage explains — for example, selling counterfeit drugs. You set up shop by creating the website and the databases, striking a deal with a bank to accept credit-card payments and creating a customer-service arm to deal with complaints — all the back-end parts of the business (see 'A tangled web').

"You don't send the spam yourself," says Savage. "You open that up to affiliates" — specialists who know how to send reams of clickable messages that fool people's spam filters. "They get 30–40% of the purchase price for any order they bring to you," he says. And if the brilliant idea turns out to be a dud — well, they just go and spam for someone else.

This affiliate business model has been confirmed in subsequent studies by Savage and many others[11], and turns out to apply to a broad range of cybercrimes, from the sale of knock-off handbags to ransomware, credit-card piracy and other forms of cybertheft. All are supported by the same underground economy of affiliate services, of which spam generation is only one. Others range from companies in India where people spend their days typing in characters from CAPTCHA symbol-recognition tests — thus 'proving' that a malicious program is human — to an up-and-coming spam alternative known as search-engine poisoning, in which people who click on legitimate-looking search results are redirected to malicious websites.

Unfortunately for law-enforcement agencies, tracing the structure of this underground economy rarely helps them to arrest the individuals involved; real-world identities tend to be closely guarded behind online pseudonyms. And in any case, the criminal cyberinfrastructure is remarkably resilient. In October 2013, for example, the FBI managed to shut down Silk Road, an eBay-like website that linked buyers and sellers for illicit commodities including hard drugs. Silk Road 2.0 appeared online a month later. And when the FBI shut down that site in late 2014, still others popped up.

However, researchers have uncovered some potentially more effective ways to attack the underground economy. Savage and his colleagues found[12] that by far the weakest



A TANGLED WEB

Recent studies have revealed that cybercriminals rely on a complex network of specialized services and affiliates. (Simplified example shown.) This introduces weaknesses that could be exploited by law-enforcement agencies.

SOURCE: REF. 11

links were the banks that processed credit-card payments to the profit centres. They were at the mercy of the credit-card companies, whose contracts generally state that any bank that represents a merchant must guarantee that a sale is legal — and is liable for paying customers back if they complain. Few banks were willing to take such risks. "It turned out that 95% of counterfeit spam on the planet went through just three banks," says Savage: one each in Azerbaijan, Latvia and St Kitts and Nevis. In November 2011, Microsoft worked with Visa to pressure those banks to drop the vendors that were pirating its products. "And for 18 months," says Savage, "there was no one selling pirated Microsoft software on the Internet."

It was not a permanent solution, however: banking support for the shady software vendors eventually moved to east Asia, where Western companies and law-enforcement agencies have considerably less leverage. Still, the hope is that continuing research will be able to make a big difference in the long run. "For the first time," says Nicolas Christin, a computer engineer who studies the human side of cybersecurity at Carnegie Mellon, "we have vast amounts of data about the underground economy."

Try that in the real world, says Christin: anyone who wanted to understand, say, the street-drug trade in Pittsburgh would have to go undercover and risk getting killed. And even then, they would get only a fragmentary, ad hoc glimpse of the whole picture.

But in the online world, every transaction leaves a digital trail, says Christin, who has led research on Silk Road — especially when payments are made using digital currencies such as Bitcoin. "And for an economist, that's wonderful." Christin and others in this field have watched criminal systems grow, mature and be taken down — and others spring up in their place. They have watched coalitions form and dissolve, and tracked how the flow of money between criminals helps them to build trust.

"We're just beginning to scratch the surface on the analysis," says Christin. But he foresees this flood of data resulting in a new fusion of computer science with social science and conventional law enforcement. "It may actually be very fruitful ground for refining and testing existing theories of criminal behaviour," he says.

Savage has a similar hope. Whether the focus is inward- or outward-looking, he says, "There is so much snake oil around security. Very few decisions are based on data." Continuing research could help people to base more of those decisions on evidence, he says. "But to do that, you have to look at the people involved — their motivations and incentives." ■

M. Mitchell Waldrop *is a features editor for* Nature *in Washington DC.*

1. *Net Losses: Estimating the Global Cost of Cybercrime* (Center for Strategic and International Studies, 2014); available at go.nature.com/15nom3
2. *IBM 2015 Cyber Security Intelligence Index* (IBM, 2015); available at go.nature.com/qcxkux
3. Bonneau, J., Herley, C., van Oorschot, P. C. & Stajano, F. *Proc. IEEE Symp. on Security and Privacy* 553–567 (2012).
4. Steves, M. *et al. Report: Authentication Diary Study* (National Institute for Standards and Technology, 2014); available at http://dx.doi.org/10.6028/NIST.IR.7983
5. Kirlappos, I., Parkin, S. & Sasse, M. A. *Proc. Workshop on Usable Security* http://dx.doi.org/10.14722/usec.2014.23007 (2014).
6. Shay, R. *et al. Symp. Usable Privacy and Security (SOUPS)* (2010); available at go.nature.com/bwuclr
7. Ur, B. *et al. ;login;* 51–57 (December 2012); available at go.nature.com/koxdc3
8. Mazurek, M. L. *et al. Proc. 2013 ACM SIGSAC Conf. on Computer & Communications Security* 173–186 (2012).
9. *Password Guidance: Simplifying Your Approach* (CESG & Centre for the Protection of National Infrastructure, 2015); available at go.nature.com/bgxre8
10. Levchenko, K. *et al. Proc. IEEE Symp. on Security and Privacy* 431–446 (2011).
11. Thomas, K. *et al. Proc. Workshop on the Economics of Information Security (WEIS)* (2015); available at go.nature.com/4emecm
12. McCoy, D., Dharmdasani, H., Kreibich, C., Voelker, G. M. & Savage, S. *Proc. ACM Conf. on Computer and Communications Security* 845–856 (2012).

THE PASSWORD GAME

Which of these passwords is stronger?
• *iloveyou88*
• *ieatkale88*
Test your password IQ at:

NATURE.COM
go.nature.com/x13ctg