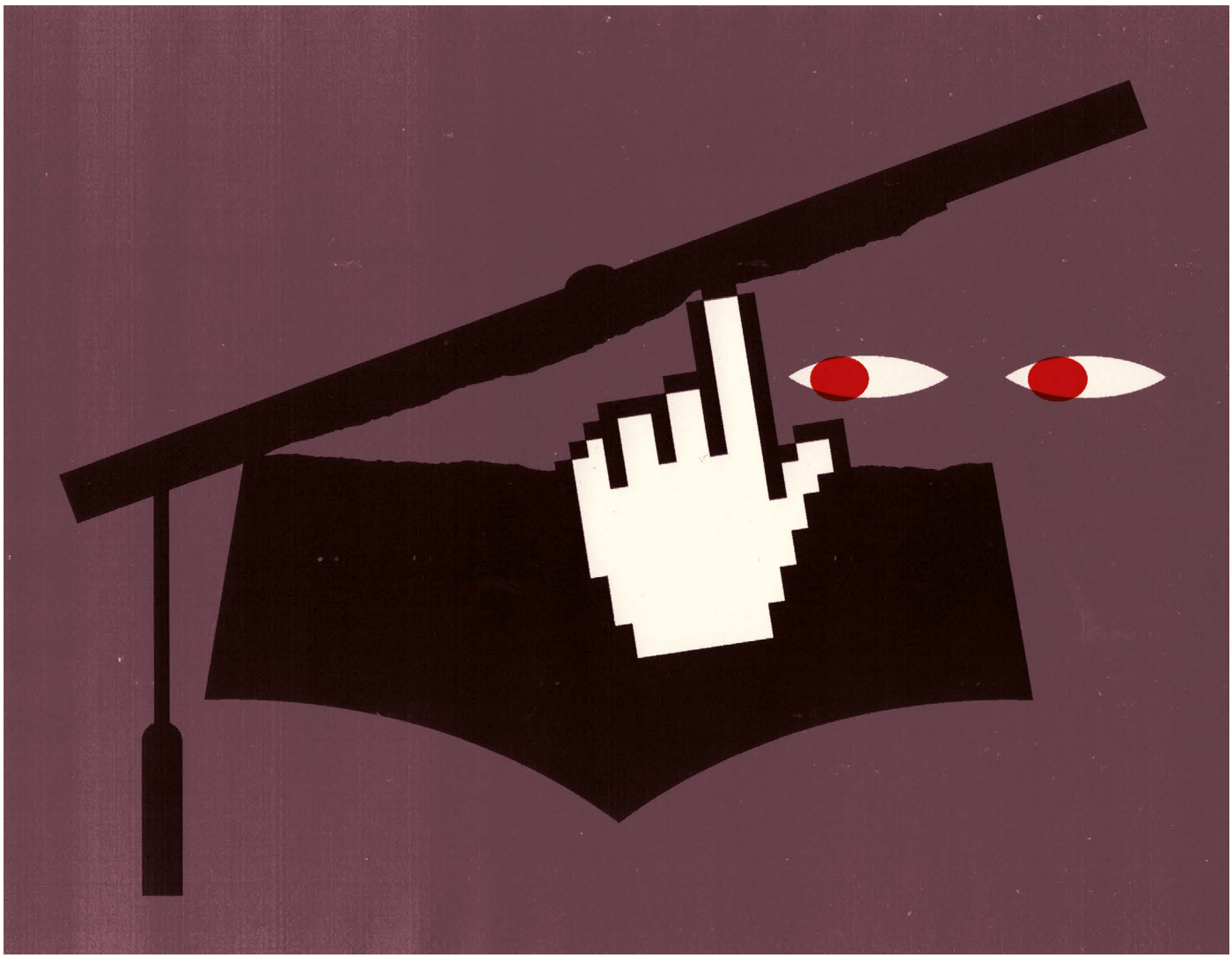

ILLUSTRATION: THE PROJECT TWINS

SO... YOU'VE BEEN HACKED

Research institutions are under siege from cybercriminals. How do you make sure you don't let them in? **By Michael Brooks**

It's every researcher's worst nightmare. A careless click on an e-mail and years of laboratory data are instantaneously encrypted by hackers. Or a piece of legacy lab equipment is compromised through its ancient, zero-security connection to the Internet. The machine might have been a godsend for running experiments from home during the COVID-19 pandemic, but now it's an open door to those who wish to exploit your institutional intranet. In this viral infection, you, embarrassingly, are patient zero.

The list of hacked academic institutions, research centres and infrastructure makes alarming reading. It includes the School of Medicine at the University of California, San Francisco (UCSF); the Fred Hutchinson Cancer Center in Seattle, Washington; the Berlin Museum of Natural History; the Atacama Large Millimeter/submillimeter Array (ALMA) telescope in Chile; the Japan Aerospace Exploration Agency in Tokyo; the University of Wollongong in Australia; and the British Library in London.

But that list hardly scratches the surface — and certainly doesn't reflect the many incursions that have been attempted. Research institutions are essentially under siege. "At the University of São Paulo, there are daily attempts to breach security protocols," says Ildeberto Aparecido Rodello, director of the Information Technology Center at the university's Ribeirão Preto campus in Brazil. The same goes for CERN, Europe's particle-physics lab near Geneva, Switzerland. "We've been lucky in the past couple of years that we haven't had any breaches which are worth calling a breach," says Stefan Lueders, CERN's head of computer security. "There are attackers outside who are constantly probing the organization for weaknesses."

It can be hard to appreciate the scale of these operations, says James Fleming, chief information officer at the Francis Crick Institute in London. "The kind of actors who perform cyberattacks at scale are hugely efficient: they

automate the vast majority of their processes," he says. "The data our firewall collects shows that bots are trying different passwords to log onto accounts and different systems, or trying to find the vulnerabilities, tens of thousands of times a week."

The problem is, universities and other research institutions can be soft targets. They thrive on data-sharing and openness and have a vast and highly mobile workforce, most of whom are less focused on cybersecurity than on the ability to access their systems from wherever they happen to be. "We're here to share research and we're open by design, which makes us weak to cybercrime," says Sarah Lawson, chief information security officer at University College London. "Education has been heavily targeted over the last few years, and the statistics tell us that that's on the rise."

What's more, she adds, universities haven't conventionally invested in cyber defence, putting them on the back foot in what she likens to "a game of whack-a-mole": eventually, you are going to lose. "It's not if," she says, "it's when."

Devastating consequences

When that happens, the consequences can be catastrophic. In a ransomware attack, for instance, precious files could be stolen or encrypted so that they cannot be accessed, unless the file owner pays the attacker. "You really have very few options," Fleming says. "You can either just wipe everything and take the hit, or you can end up with a financial penalty." UCSF took the second option after a 2020 breach of their systems, choosing to pay a ransom of US$1.14 million.

But if everything is backed up and no sensitive data have been compromised, the first option might not be too bad, Fleming says. "You hard-wipe all the machines and reformat all the hard drives, and then you do a rebuild. You maybe lose a week of productive time."

That does depend on the scale of the attack and the preparedness of your institution, however. The British Library is now performing a "full technical rebuild and recovery" on its digital infrastructure after an October 2023 cyberattack, which occurred as the library was updating its core technology infrastructure. "The work will now be accelerated," a spokesperson told *Nature*. It's too early to say how long that will take or what it will cost, they add, but *The Financial Times* has estimated a price tag of around £7 million (US$9 million).

Recovering from the attack on the ALMA observatory, which happened in October 2022, took "a bit less than seven weeks", according to Jorge Ibsen, head of ALMA's computing department. But the financial hit can only be guessed at, he says. "The best estimate would be 13% of the annual operational cost, which is the fraction of days within a year we could not deliver to our mission." As for details of what the recovery entailed, and the measures taken since, Ibsen is keen to keep them under wraps. "Given the nature of this threat, we cannot further discuss details about our specific cybersecurity strategy," he says.

Institutional cyberattacks don't always end with a ransom payment or rebuild of digital infrastructure. For one thing, paying a ransom doesn't necessarily preclude bad actors from weaponizing or releasing data. And there could be legal repercussions. For instance, some people who were affected by the attack at the Fred Hutchinson Cancer Center, in November 2023, have filed class-action lawsuits against the centre.

Unplug and shut down

What about the individuals who are compromised? When it happens to you, what should you do? Unanimously, these heads of cybersecurity plead that you communicate with them — after turning off and disconnecting whatever device has been hacked. "Pull out the plugs and shut it down. Close it and then seek advice," Lawson says.

"Cybercriminals will use every technique in the book to find the way into your money."

That said, prevention is always better than cure, and a properly prepared human can be a powerful firewall. "Update your software regularly; implement firewall and antivirus solutions; control access and permissions to your systems; encrypt sensitive data," Rodello says. He even suggests engaging cybersecurity specialists to conduct regular audits and provide guidance on improving your lab's digital safety.

After all, most academics are not trained IT professionals, and DIY solutions can be dangerous. Lawson says she can't help but admire cybercriminals' ability to manipulate their targets. "They're the best psychologists in the world," she says. "They will use every technique in the book to find the way into your money. And they're really good at it."

It might seem obvious, but another tip is to back up data somewhere secure — and, if possible, somewhere off-site. And don't overlook the software you wrote yourself. "Ideally, people use proper software libraries and they run tests to make sure of its security," Lawson says. "But we do have problems with people who don't think about that." Great researchers, she appreciates, are rarely focused on the fact that many criminals are out to ruin their lives.

Evolving threats

Those working in the health-care sector are at especially high risk. "The health-care system currently is one of the number-one targets for hacking because of the financial benefit that people can gain from getting a health record," says Anthony Cartwright, an anaesthesiologist at the Cleveland Clinic in Abu Dhabi, United Arab Emirates, who has written about the cybersecurity risks in health care (A. J. Cartwright *J. Clin. Monit. Comput.* **37**, 1123–1132; 2023).

Some vulnerabilities arose during the COVID-19 pandemic, Cartwright says, when many hospital staff began working from home. In many cases, those systems have not been updated. "They're now accessing hospital network systems on an unsecured personal network. Often, that computer in the house will be shared between the mum, dad, brother or sister." In other words, anything could get on there.

Such systems need to be updated, of course. But don't overlook common-sense precautions, such as keeping passwords private. Cartwright was struck by a television segment filmed in a hospital during the pandemic. "As the camera panned around to one of the nurses at the control desk, there was a piece of paper giving the password — and you could read it on screen," he says. "The Wi-Fi password was right there, on TV."

That said, thanks to government initiatives such as the 1996 US Health Insurance Portability and Accountability Act (HIPAA), healthcare workers are often more security-savvy than are academic researchers, reckons Anton Dahbura, executive director of Johns Hopkins University's Information Security Institute in Baltimore, Maryland. "It's much more top of mind and it's been instilled in the culture."

At the same time, however, bad actors are getting more sophisticated. Although some hacks are for sport or to advance a political agenda — hacktivists targeting scientists working on controversial research, for instance — cybersecurity professionals are increasingly concerned about state-level actors whose aim is to destabilize critical infrastructure or steal intellectual property. "Universities hold a lot of important, proprietary and sensitive information," Dahbura says. Scientific research institutes such as genomics labs "hold information that adversaries, in particular nation states, would love to have", he points out. "It's no different than hacking into a research and development lab of a pharmaceutical company, except that it's probably easier at a university."

Whatever the motivation, no one wants to be the one who let an attacker in. Lueders offers a simple mantra: "Stop, think, don't click!" This is how you prevent the majority of hacking attempts, he says. "The Internet has made us all so curious that we click on things without knowing what they are. The brain can be really stupid."

Michael Brooks is a science writer in Lewes, UK.