TOOLBOX

CYBERSECURITY FOR THE TRAVELLING SCIENTIST

Virtual private networks, tracking apps and 'burner' laptops: how to protect sensitive data when you take your research on the road.

ILLUSTRATION BY THE PROJECT TWINS

BY BRIAN OWENS

Mark Gerstein has had his fair share of scares when it comes to losing track of his electronic devices — and, along with them, access to his private information and research data.

"I'm very security conscious, but also a bit of an absent-minded professor," says Gerstein, a bioinformatician at Yale University in New Haven, Connecticut.

He recalls one trip to Boston, Massachusetts, when he left his phone in a taxi, and watched it get farther and farther away on the tracking app on his iPad while he ran after the car in vain. Luckily, Gerstein was able to contact the taxi company, and eventually watched his phone make the return journey to his pocket.

Gerstein's story had a happy ending, but all too often, hardware lost on the road is lost for good. And that's just one of the many threats travelling researchers must face. Outside the confines of the lab and its relatively secure IT infrastructure, data and hardware are vulnerable to dangers such as hacking and theft. Researchers need to be on their guard, not just to protect their work, but also to protect confidential patient data or intellectual property.

Cybersecurity concerns can be particularly acute when crossing international borders. Some regions have a reputation for hacking, and border guards might insist on seeing files.

What can researchers do to keep their ▶

▸ data safe from prying eyes on the road? It depends on your data and the threats you're likely to face, says Morgan Marquis-Boire, director of security for First Look Media in San Francisco, California, who has experience helping government whistle-blowers travel with sensitive data. Are you concerned mostly about overzealous border guards, opportunistic theft or government-sponsored hacking?

It's like chatting with a physician, he says. "If you ask a doctor how to be healthy, you'll get general advice. But it will be different if you're going to the jungle."

Whatever the perceived threat, the first step in data protection, says Marquis-Boire, is encryption — rendering data unreadable by mathematically transforming them with an electronic key (see 'Dos and don'ts'). This simple step can protect against casual theft and deter all but the most determined hackers. "The number one thing we push for is encryption of data, whole-disk encryption of portable devices especially," says John Southall, a data librarian at the University of Oxford, UK.

Most smartphones use whole-disk encryption by default, and there are many options for encrypting laptops. Particularly sensitive files should also be individually encrypted using the computer's built-in file-protection tool or freely available software such as VeraCrypt, BitLocker or 7-Zip. Your research institution may be able to help. Oxford's information-security department, for instance, will encrypt researchers' hardware. "We have an understanding of not only the necessary protections for research data, but also researchers themselves," says Southall.

LOST PROPERTY

Researchers must also consider the physical security of their electronic devices, adds Southall. "Laptops and other devices are high-value items. They attract theft. So make sure whatever is on them is not irreplaceable."

A tracking app capable of remotely wiping a lost laptop or phone (such as Apple's Find My iPhone) can ensure that even if hardware is taken, data are not compromised, says Gerstein.

A US ban on carrying laptops in the cabin on flights from various Middle Eastern airports, announced on 21 March, has introduced a new complication, says Jonathan Katz, who studies cybersecurity at the University of Maryland in College Park. "It's greatly increased the risk of your laptop being damaged, lost or stolen, and your data compromised." There is a similar ban in the United Kingdom, but may soon be lifted.

Katz will soon be travelling to the Middle East for work. Although he will not be carrying anything particularly sensitive, he plans to ship the computer home using FedEx, rather than leaving it unattended in his checked baggage if the US ban is still in place.

Dos and don'ts

- Do get help and advice from your institution before you travel.
- Do encrypt your data at both the whole-disk and file level.
- Do use a virtual private network for remote networking.
- Don't carry data on USB sticks. They are easy to lose, rarely encrypted and difficult to erase completely.
- Do log out of cloud-based services, uninstall the apps and clear your browser history.
- Do consider a 'burner' laptop and phone for use while travelling.
- Don't leave your laptop or phone unattended in your car or hotel room. B.O.

SAFETY IN THE CLOUD

In many cases, tech-savvy researchers can avoid carrying their data at all. The data can be archived in cloud services such as Dropbox or Google Drive, and accessed from the researcher's destination. Although these services are encrypted and relatively secure, researchers should also encrypt files before uploading them in case the servers are hacked, or their account password is compromised. (Two-factor authentication, in which both a password and mobile-phone-generated key are required to access your account, adds an extra layer of security.)

Because these services are often set up to provide automatic access, Marquis-Boire advises researchers travelling internationally to remove the app from their devices, log out of the service and clear their browser history before travel.

Researchers should also consider using a virtual private network (VPN), says Southall. These allow users to establish secure network communications over an otherwise insecure Internet connection. Such services include IPVanish VPN, NordVPN and the colourfully named Hide My Ass, and many institutions can provide assistance in setting them up, he says.

Gerstein notes he almost always uses a VPN to access his data when travelling, even when he isn't leaving the United States. In most places, a VPN is fairly easy to use, although it can get more complex in countries where the government exerts tight control over the Internet, such as China. Although VPNs are legal there, the government launched a crackdown on domestic VPN providers in January this year. It is not clear, however, what effect this will have on the overseas VPNs that researchers are likely to use.

For many scientists, travel to China tops their list of mobile cybersecurity concerns, leading some to take extra precautions. The country has faced allegations of using cyber-espionage to speed technological advances (the US steel industry, for instance, accused Chinese hackers of stealing trade secrets in 2016), and has been accused of hacking researchers and scientific institutions in the past, including a 2014 cyberattack on Canada's National Research Council. Stephen Kingsmore, president of the Rady Children's Institute for Genomic Medicine in San Diego, California, says that some of his colleagues use a 'burner' laptop and phone (low-cost, disposable devices) when travelling to China.

BORDER TROUBLES

In the past year, a new threat to data security has arisen for travellers, as the administration of US President Donald Trump works to harden US borders against potential terrorists. Border agents may sometimes ask travellers to provide their portable devices and passwords when they enter the country, and such searches are increasing. US National Public Radio reports that 24,000 devices were searched at the border in 2016, compared with 8,500 in 2015.

Researchers are not exempt from this heightened scrutiny. As was widely reported in March, Sidd Bikkannavar, a US citizen and engineer at NASA's Jet Propulsion Laboratory (JPL) in Pasadena, California, was detained at the airport in Houston, Texas, while returning from a personal trip to South America. He was forced to hand over his NASA-issued phone and PIN. Citing the confidential data on the device, Bikkannavar initially refused, but ultimately relented. His phone was taken for 30 minutes and its data copied. Back at JPL, NASA had to run forensic tests on the device to determine what might have been taken, and whether anything had been installed. (Bikkannavar could not be reached for comment, and JPL declined to discuss its cybersecurity arrangements.)

It can be tempting to try to hide information or use technological tricks such as 'duress passwords' that, if used instead of the genuine one, unlock the device but keep a portion of the data hidden and encrypted. But Jennifer Granick, who studies cybersecurity law at Stanford University in California, warns against such strategies. "You don't want to lie to a government agent. That can be a crime." And border guards are not likely to be sympathetic to the argument that a researcher has a legal duty to prevent anyone from seeing confidential data.

"Medical records, trade secrets — there are a lot of data that you have a legal obligation to protect. Border agents are not experts in these areas of law, they're not going to necessarily care about that," Granick says. "So you have to think about how you're going to protect your data." ■

Brian Owens *is a freelance writer based in New Brunswick, Canada.*

CORRECTION

The Toolbox article 'Single-cell sequencing made simple' (*Nature* **547,** 125–126; 2017) omitted the first name and affiliation of John Marioni from Cancer Research UK. Furthermore, the name of FlowJo's software is SeqGeq, not GenSeq.