pulses of infrared light for analysing proteins and nucleic acids in blood samples from people with cancer. The aim will be to find molecular ‘fingerprints’ that might diagnose cancers, or predict response to therapy or the future onset of a cancer.

The value of such a source of infrared light, Krausz says, is that a table-top-size laser system could be developed and used at patients’ bedsides. Currently, the only sources of such radiation are synchrotrons, which require large, expensive infrastructures. Because Krausz has little experience in this area, it would have been hard for him to obtain funding in Germany for such medical applications, he says.

“They provide an exquisitely sharp temporal scalpel for dissecting the inner workings of matter.”

The place of women in Saudi society and education, and the country’s human-rights record, have presented challenges for members of the collaboration. At KSU, which was founded in 1957, male and female students have separate campuses. No rule forbids women from entering the new lab, says Abdallah Azzeer, who leads the KSU side of the laser collaboration, but mixing of the sexes contravenes cultural norms. “We will make special arrangements to ensure their access,” he says. One possibility, he adds, might be to train female PhD students in handling the equipment so that they can supervise female undergraduates whose parents do not want them to attend mixed classes.

Krausz has had to get used to working in a segregated environment during his time at KSU. All the lectures are given in the men’s campus and beamed over to the women’s campus, and Krausz remembers being extremely startled the first time he received a disembodied question from a female student over loudspeakers.

He thought long and hard about working with Saudi Arabia, he says. As a Hungarian who left for the West in 1987 at the age of 25, he is hypersensitive to human-rights issues. But not long before he decided to collaborate with KSU in 2008, he had cancelled a trip to China in protest against a clamp-down on press freedom there, and then regretted the decision. It achieved nothing save the embarrassment of the scientists, he says, and he concluded that, in such cases, “the best thing is to talk to each other and learn each other’s problems”.

He found himself genuinely moved by the enthusiasm for science he encountered on his first visit to KSU later that year. “It felt like a small revolution was happening,” he says. “I thought about how I would have felt in the same situation in Hungary — I might have stayed.” ■

US President Barack Obama has ordered better federal cooperation with private firms to fight hackers.

NICHOLAS KAMM/AFP/GETTY

CYBERSECURITY

Cybercrime fight targets user error

Researchers consider ways to diminish human factors in the equation for keeping data safe.

BY ERIKA CHECK HAYDEN

It would be easy to blame the poor soul at Sony Pictures Entertainment who opened the door to one of the most disastrous hacks in history just by clicking an e-mail link. As US President Barack Obama pointed out during a visit to Stanford University in California on 13 February, user negligence is often the key to a successful cyberattack.

“It’s just too easy for hackers to figure out usernames and passwords, like ‘password’. Or 12345 … 7,” Obama said. But people do this kind of thing all the time, says Angela Sasse, head of information-security research at University College London. Researchers have found that after employees were asked to create long passwords according to strict rules, some of them wrote the password down in an easily accessible place, such as on a desk in plain sight. Other employees might choose to work outside a secured network because it runs too slowly (see also go.nature.com/buxsds).

Such measures confound security experts but are a logical response to the increasing security workload imposed on employees, Sasse says. “We want security that is effective but also allows us to get on with the job,” she adds. “A lot of smarter companies are realizing that some of these security measures are a bad productivity drain.” Cormac Herley, a security researcher at Microsoft Research in Redmond, Washington, has estimated that the world’s Internet users collectively spend the equivalent of 1,389 years every day entering passwords (C. Herley *IEEE Secur. Priv.* **12,** 14–19; 2014).

Generally, the financial services industry is further ahead than others in dealing with the problem, because its business relies on ensuring that customers can easily access their funds while thieves are kept out. But a spectacular failure in its efforts was revealed on 16 February, when the Russian computer-security firm Kaspersky Lab described how hackers had managed to steal an estimated US$1 billion from financial institutions around the world by infiltrating a bank in Ukraine. As in the Sony case and many others, the fatal security flaw was an errant click on an e-mailed link.

In banking, authentication is the key step

— verifying that someone trying to access funds in a customer's name is the actual customer. This is increasingly done through layers of multiple passwords that must meet rules on length and complexity, making them hard to enter correctly on mobile devices, for example.

Some banks are experimenting with ways to jettison passwords altogether. In 2013, major German banks deployed a system called photoTAN that uses an application downloaded to a phone or desktop computer to ensure that only customers can see e-mailed account information and that hackers cannot send counterfeit e-mails. The system mathematically encodes transaction information into an image that looks to a hacker or any other observer like a meaningless jumble of coloured squares. But when a customer with the application snaps a photo of the image, it is decoded to reveal the transaction information.

A project by Google aims to revamp a system known as CAPTCHA, which distinguishes humans from programs called bots that can be used in various malicious ways, such as harvesting e-mail addresses. The existing CAPTCHA format asks a computer user to retype a line of distorted text to make the distinction, but as artificial intelligence has advanced, the text distortion has increased such that it often defies humans as well as machines. Google's project aims to make this verification process less painful, and even invisible.

In December, Google deployed a system that, according to the company's online-security blog, "considers a user's entire engagement with the CAPTCHA — before, during, and after — to determine whether that user is a human". Google has not specified what that means, but it is believed to involve tracking a person's browser history and spotting distinctively human cues in how the cursor moves to the text box, for instance. In some cases, the program can verify that a user is human without the person even completing the task.

Another effort being spearheaded by Google, along with the file-hosting service Dropbox and the Open Technology Fund in Washington DC — an organization funded by the US government to foster free speech online — aims to improve user experience to make e-mail encryption easier. There are two existing programs, Pretty Good Privacy (PGP) and GNU Privacy Guard (GPG), which are 'open source' and so can be used by anyone to make e-mail completely indecipherable to those who might intercept it. The systems are safe and effective: whistle-blower Edward Snowden specifically chose to leak US National Security Agency documents to documentary film-maker Laura Poitras because she uses encryption software. He knew that he could communicate with her without fear of anyone eavesdropping.

But these systems are difficult to use, so many people do not. That makes it much easier for cybercriminals to entice people to click on links, especially in the increasingly distracting online world. Google and its partners have helped to establish a non-profit online privacy consultancy called Simply Secure, which is now helping developers of such open-source programs to improve the experience for users. If the effort succeeds, the practice of using counterfeit e-mails to lure people into clicking malicious links could become much less prevalent.

But just as in conventional conflicts, the war against hackers is an arms race. "We design new defences, and then hackers and criminals design new ways to penetrate them," Obama said at Stanford. "So we've got to be just as fast and flexible and nimble in constantly evolving our defences." ■

CAREER DEVELOPMENT

Young scientists go for fresh ideas

Analysis of millions of papers finds that junior biomedical researchers tend to work on more innovative topics than their senior colleagues do.

BY EWEN CALLAWAY

Bad news, scientists: there is a good chance that your most cutting-edge work is behind you.

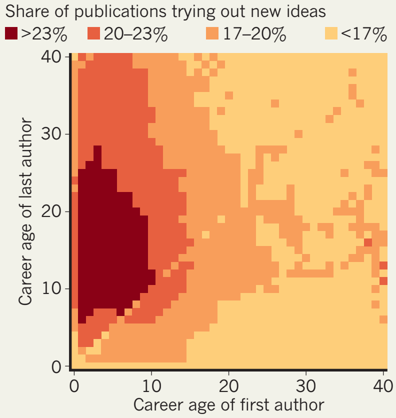
Young researchers are much more likely than older scientists to study exciting innovative topics, according to a text analysis of more than 20 million biomedical papers published over the past 70 years. More-senior researchers are more likely to publish in hot areas when they are supervising a younger scientist.

Researchers are at their most creative when they are young, or so says conventional wisdom: Charles Darwin and Max Planck both argued that young scientists were more open than older colleagues to new ideas. But the topic is not just fodder for chats over post-seminar beers. Funders such as the US National Institutes of Health have implemented policies specifically to support early-career scientists, based in part on the view that young researchers are more innovative than seasoned scientists. And in mathematics, the Fields Medal has been reserved for researchers under 40.

"It's always just a claim — the young are more innovative — but there's no proof," says Mikko Packalen, an economist at the University of Waterloo in Canada, who led the study with economist Jay Bhattacharya of Stanford University in California. Their working paper was published this month by the US National Bureau of Economic Research (M. Packalen and J. Bhattacharya Preprint at http://doi.org/z87; 2015).

HOT SPOT

Pairings of young first authors and mid-career last authors are the most likely to work on the hottest biomedical topics.



SOURCE: M. PACKALEN & J. BHATTACHARYA PREPRINT AT HTTP://DOI.ORG/Z87 (2015)

To determine which scientists used the most innovative ideas, Packalen and Bhattacharya turned to the leading index of biomedical research, MEDLINE (accessed through the website PubMed), which stores more than 21 million articles published since 1946.

The duo developed a computer program that identifies every one-, two- or three-word string in the title and abstract of each paper. It then logs when each string first appeared in the literature and counts how many times it has appeared subsequently, to determine its popularity. (The all-time winning concept was 'polymerase chain reaction', the DNA-copying technique, occurring in more than 176,000 titles or abstracts.)

Packalen and Bhattacharya then ranked the most innovative articles for each year, from 1946 to 2011, on the basis of whether they were an 'early adopter' of the hottest keywords.

The method could not measure researchers' creativity, only their willingness to ►