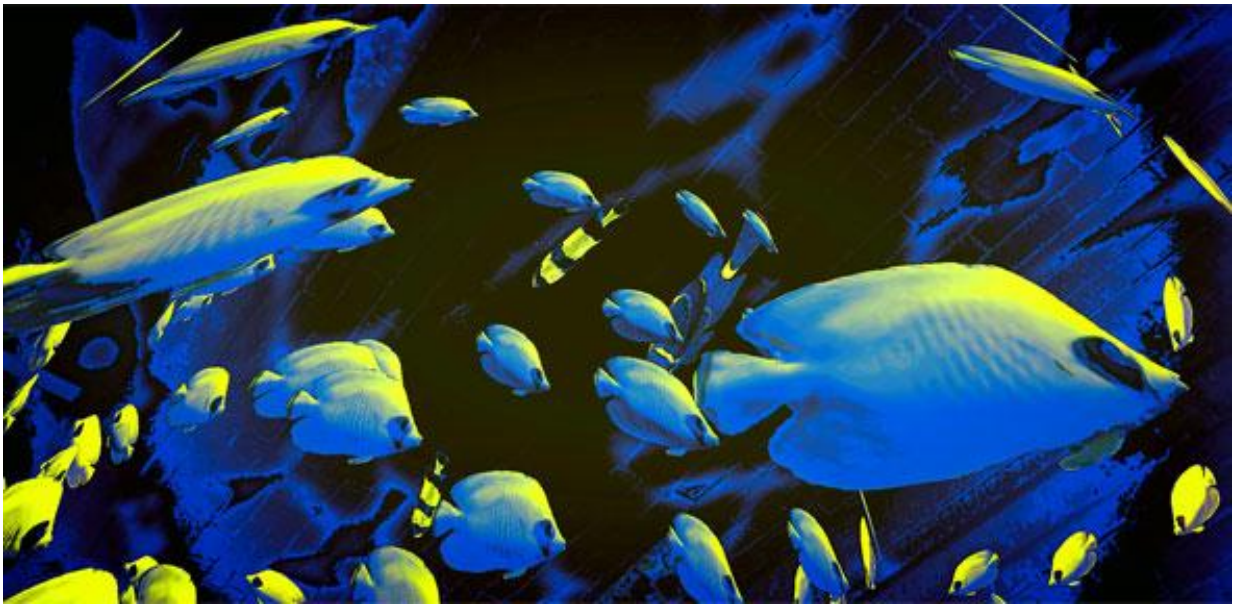
Combating cybercrime when there's plenty of phish in the sea

October 21 2016



TeQi's Graffitti Phish. Credit: LastHuckleBerry

As more and more crime moves online, computer scientists, criminologists and legal academics have joined forces in Cambridge to improve our understanding and responses to cybercrime, helping governments, businesses and ordinary users construct better defences.

We've all received the emails, hundreds, maybe thousands of them. Warnings that our bank account will be closed tomorrow, and we've only

got to click a link and send credit card information to stop it from happening. Promises of untold riches, and it will only cost a tiny fee to access them. Stories of people in desperate circumstances, who only need some kind soul to go to the nearest Western Union and send a money transfer to save them.

Tricking people into handing over sensitive information such as credit card details – known as 'phishing' – is one of the ways criminals scam people online. Most of us think we're smarter than these scams. Most of us think that we could probably con the con artist if we tried. But we would be wrong.

Across the world, cybercrime is booming. When the UK government included cybercrime in the national crime statistics for the first time in 2015, it doubled the crime rate overnight. Millions of people worldwide are victimised by online scams, whether it's blocking access to a website, stealing personal or credit card information, or attempting to extort money by remotely holding the contents of a personal computer hostage.

"Since 2005, the police have largely ignored cybercrime," says Professor Ross Anderson of Cambridge's Computer Laboratory. "Reported crime fell by as much as a half in some categories. Yet, now that online and electronic fraud are included, the number of reported crimes has more than doubled. Crime was not falling; it was just moving online."

In 2015, computer scientists, criminologists and legal academics joined forces to form the Cambridge Cybercrime Centre, with funding from the Engineering and Physical Sciences Research Council. Their aim is to help governments, businesses and ordinary users to construct better defences.

To understand how the criminals operate, researchers use machine learning and other techniques to recognise bad websites, understand what

kinds of brands tend to be attacked and how often, determine how many criminals are behind an attack by looking at the pattern of the creation of fake sites and how effective the various defence systems are at getting them taken down.

One way in which studying cybercrime differs from many other areas of research is that the datasets are difficult to come by. Most belong to private companies, and researchers need to work hard to negotiate access. This is generally done through nondisclosure agreements, even if the data is out of date. And once researchers complete their work, they cannot make the data public, since it would reduce the competitive advantage of corporate players, and it may also make it possible for criminals to reverse engineer what was detected (and what wasn't) and stay one step ahead of law enforcement.

One of the goals of the Cambridge Cybercrime Centre is to make it easier for cybercrime researchers from around the world to get access to data and share their results with colleagues.

To open up cybercrime research to colleagues across the globe, the team will leverage their existing relationships to collect and store cybercrime datasets, and then any bona fide researcher can sign a licence with the Centre and get to work without all the complexity of identifying and approaching the data holders themselves.

"Right now, getting access to data in this area is incredibly complicated," says Dr Richard Clayton of Cambridge's Computer Laboratory, who is also Director of the Centre. "But we think the framework we've set up will create a step change in the amount of work in cybercrime that uses real data. More people will be able to do research, and by allowing others to work on the same datasets more people will be able to do reproducible research and compare techniques, which is done extremely rarely at the moment."

One of the team helping to make this work is Dr Julia Powles, a legal researcher cross-appointed between the Computer Laboratory and Faculty of Law. "There are several hurdles to data sharing," says Powles. "Part of my job is to identify which ones are legitimate – for example, when there are genuine data protection and privacy concerns, or risks to commercial interests – and to work out when we are just dealing with paper tigers. We are striving to be as clear, principled and creative as possible in ratcheting up research in this essential field."

Better research will make for better defences for governments, businesses and ordinary users. Today, there are a lot more tools to help users defend themselves against cybercrime – browsers are getting better at recognising bad URLs, for example – but, at the same time, criminals are becoming ever more effective, and more and more people are getting caught in their traps.

"You don't actually have to be as clever as people once thought in order to fool a user," says Clayton when explaining how fake bank websites are used to 'phish' for user credentials. "It used to be that cybercriminals would register a new domain name, like Barclays with two Ls, for instance. But they generally don't do that for phishing attacks anymore, as end users aren't looking at the address bar, they're looking at whether the page looks right, whether the logos look right."

The Centre is also looking at issues around what motivates someone to commit cybercrime, and what makes them stop.

According to Dr Alice Hutchings, a criminologist specialising in cybercrime, cybercriminals tend to fall into two main categories. The first category is the opportunistic offender, who may be motivated by a major strain in their lives, such as financial pressures or problems with gambling or addiction, and who uses cybercrime as a way to meet their goals. The second type of offender typically comes from a more stable

background, and is gradually exposed to techniques for committing cybercrime through associations with others.

Both groups will usually keep offending as long as cybercrime meets their particular needs, whether it's financial gratification, or supporting a drug habit, or giving them recognition within their community. What often makes offenders stop is the point at which the costs of continuing outweigh the benefits: for instance, when it takes a toll on their employment, other outside interests or personal relationships.

"Most offenders never get caught, so there's no reason to think that they won't go back to cybercrime," says Hutchings. "They can always start again if circumstances in their lives change.

"There is so much cybercrime happening out there. You can educate potential victims, but there will always be other potential victims, and new ways that criminals can come up with to social engineer somebody's details, for example. Proactive prevention against potential offenders is a good place to start."

Criminologist Professor Lawrence Sherman believes the collaboration between security engineering and criminology is long overdue, both at Cambridge and globally: "Cybercrime is the crime of this century, a challenge we are just beginning to understand and challenge with science."

"We're extremely grateful to the people giving us this data, who are doing it because they think academic research will make a difference," says Clayton. "Our key contribution is realising that there was a roadblock in terms of being able to distribute the data. It's not that other people couldn't get the data before, but it was very time-consuming, so only a limited number of people were doing research in this area – we want to change that."

"Our Cybercrime Centre will not only provide detailed technical information about what's going on, so that firms can construct better defences," says Anderson. "It will also provide strategic information, as a basis for making better policy."

Provided by University of Cambridge