Lockdown helps fuel rise in cybercrime

June 3 2020

Credit: Philipp Katzenberger on Unsplash

Take extra care before buying face masks or testing kits online, or responding to texts apparently sent to you by the UK government or the NHS. Because while lockdown has helped reduce the spread of the coronavirus, it is also helping fuel a rise in cybercrime.

That's the warning from a team of researchers including Dr. Ben Collier from the Cambridge Cybercrime Centre, part of Cambridge's Department of Computer Science and Technology.

The researchers have been analyzing data collected by the Centre from underground forums, chat channels and marketplaces used by cybercrime communities. And in a briefing paper they have just written for Police Scotland, they say it indicates that the social changes put in place in response to the coronavirus pandemic "have stimulated… the cybercrime economy."

Some of the cybercrimes taking place are new. For example, early in the lockdown, some scammers sent fake texts, purporting to come from HM Revenue & Customs, telling recipients they were going to be fined £250 for leaving their homes more than once a day.

And the researchers are also concerned that the rollout of the prospective NHS contact tracing app has the potential to generate clear risks for those vulnerable to fraud. They warn that such people may be conned into handing over sensitive personal information by fake apps or scam texts purporting to be from the NHS.

"We're also seeing some general repurposing of existing cybercrime," said Collier. "For example, there have long been fake online shops, but now instead of selling clothes, they are selling face masks or bogus 'cures' for the coronavirus."

And meanwhile, there has been a general rise in the levels of cybercrime. The Cambridge Cybercrime Centre has tracked a three-fold increase in 'denial of service' attacks from around 12,000 per day to close to 30,000 attacks per day. These attacks—which can be purchased for small amounts of money from specialized online services—can be used to knock others offline, often opponents in online games.

Such attacks, the report says, have serious implications beyond being a nuisance for gamers, as many of these children and young people will be sharing Internet connections with siblings engaged in online or blended

learning and parents working from home.

We are vulnerable to such risks, Collier and his colleagues say, because we are spending much more time online as we work, or school our children, from home. And it is partly happening because "many internet users, including adolescents and young adults, are currently confined to home with no school or work for much of the day. The increased boredom they feel may well be a key driver of online petty crime."

"Anxiety over serious economic problems—such as job losses and business closures—may be prompting some people to step up existing harmful online activity as a means of generating income," said Collier.

In their paper, the research team—Dr. Collier, Dr. Shane Horgan from Edinburgh Napier University, Dr. Richard Jones from the University of Edinburgh and Dr. Lynsay Shepherd from Abertay University—also voice their concerns about the potential for a steep rise in the volume of other online harms. These include online bullying, stalking and harassment of minority groups and victims of domestic abuse.

Their paper is a rapid response briefing aimed at offering guidance on the policing of cybercrime to Police Scotland. But its findings have relevance across the UK.

It says that while the UK has a sophisticated cybersecurity apparatus particularly at the national level, it currently lacks sufficient capability at the local level to police a significant increase in 'volume' cybercrime offenses.

And it recommends that with levels of such crimes increasing, police forces need to engage more with their local communities and work with them on measures to prevent such crimes.

The paper also recommends that police forces, including Police Scotland, immediately undertake a wide-ranging review of their cybercrime policing and prevention practices and capabilities to assess their current adequacy and potential future resilience in the event that the number of cybercrime offenses increases significantly in the near future.

More information: The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations: www.sipr.ac.uk/assets/files/REiP%20-%20Pandemic%20Cyber%20-%20Collier_Horgan_Jones_Shepherd.pdf

Provided by University of Cambridge