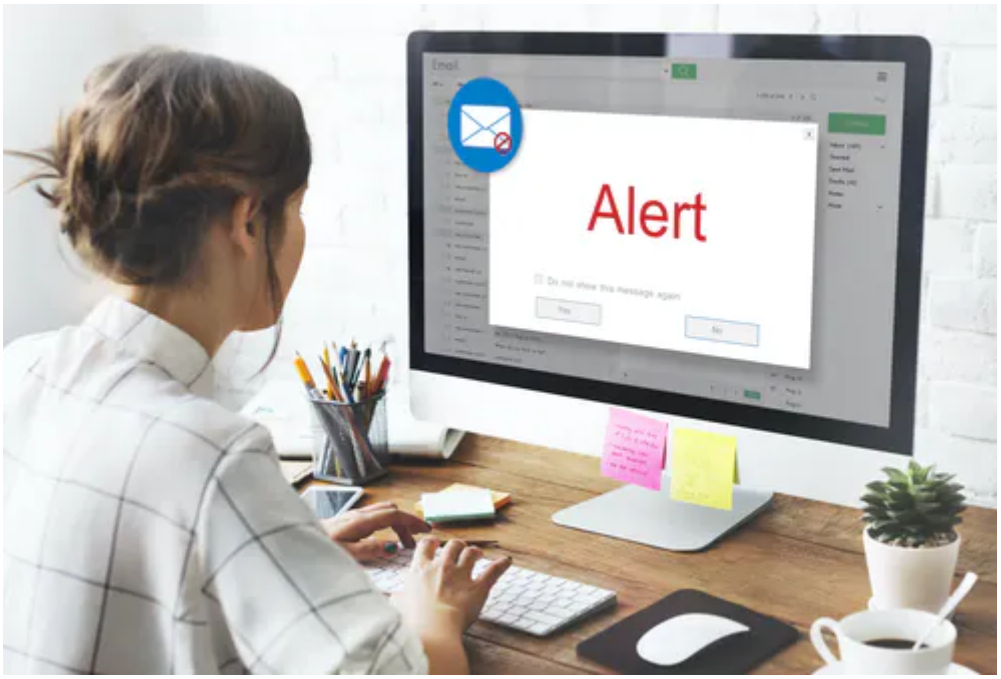
THE CONVERSATION

Academic rigour, journalistic flair



Rawpixel.com/Shutterstock

RMIT attack underlines need to train all uni staff in cyber safety

March 1, 2021 6.06am AEDT

Cyber criminals are very persistent and the daily numbers of cyber attacks show no sign of decreasing. The latest reported attack on an Australian university has disrupted the start of the semester at RMIT. The suspected phishing attack – luring the recipient of an email or other communication into inadvertently giving the attacker access to the IT system – highlights the need for cyber hygiene training for all staff.

The flexible working practices and roll-out of a remote workforce culture during the COVID-19 pandemic have been a challenge for cyber security at even the most prepared organisations. The spike in cyber attacks on organisations that have had to adapt quickly to the new normal just adds to the uncertainty and fears created by the pandemic.

Authors

Abu Barkat ullah

Associate Professor of Cyber Security, University of Canberra

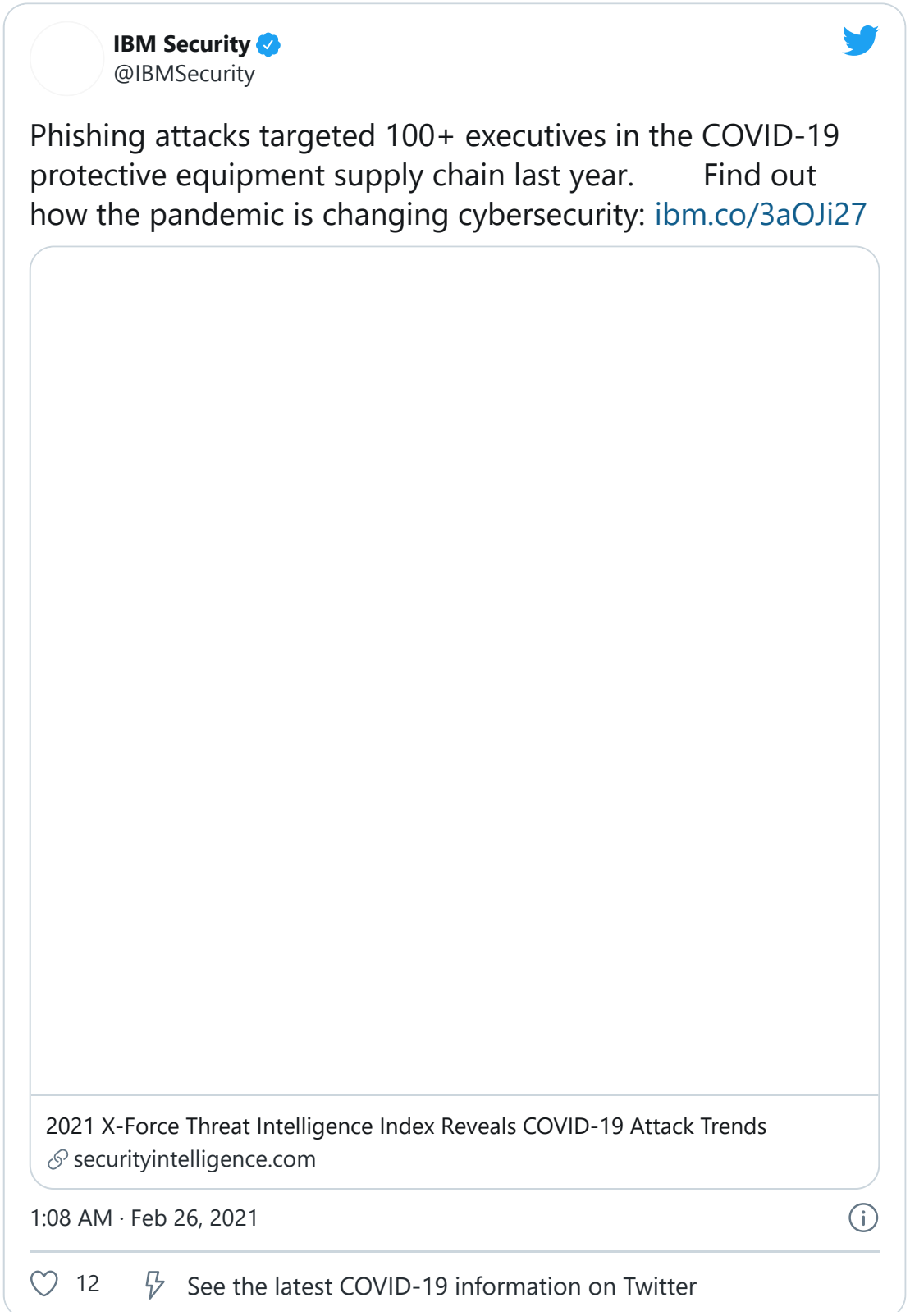
Mohiuddin Ahmed

Mohiuddin Ahmed is a Friend of The Conversation.

Lecturer of Computing & Security, Edith Cowan University

Read more:* *'Click for urgent coronavirus update': how working from home may be exposing us to cybercrime

---



Academics have access to a vast range of sensitive information. It includes student profiles, academic records, research data and other intellectual property. If computer systems or even authentication data such as login details are compromised, it's just a matter of time before cyber criminals exploit all that private information in several ways.

Universities put themselves at risk

Despite this threat, almost half of Australia's top 20 institutions in the QS World University Rankings 2020 appear to have had no protection in place against hackers trying to trick people to take over their computer systems. An analysis by cyber security firm Proofpoint found only two universities were actively blocking fraudulent emails from reaching students, alumni and faculty staff.

Cyber attacks can jeopardise the reputation of students and academics as well the institution itself. In addition to individual hackers, state-based actors are out to win the intellectual property war.

The latest Notifiable Data Breaches Report from the Office of the Australian Information Commissioner (OAIC) shows data breaches resulting from human error accounted for 38% of notifications in the second half of 2020. That's 18% more than in the past. Education is one of the top five sectors for data breaches.

This highlights how important it is that universities provide cyber safety training for all academics working in areas other than cyber security, IT or the like.

Inside a massive cyber hack on Australian National University.

Read more:* *19 years of personal data was stolen from ANU. It could show up on the dark web

3 ways staff and students can protect themselves

1. Use multi-factor authentication

Universities are making greater use than ever before of learning management platforms such as BlackBoard, Canvas, Moodle and so on to deliver online content. During their design, cyber security

was not high on the agenda. However, most learning management systems (LMS) have the option of multi-factor authentication (MFA).

This typically requires a combination pin and secret questions. These days face detection and fingerprints are also used. For example, Canvas offers two options: SMS (text) or an authenticator app to support MFA.

This adds an extra layer of security. But, in reality, few students or academics use this option consistently.

This improves cyber criminals' chances of penetrating their accounts with simple brute-force approaches, such as logically guessing credentials, or using social engineering, such as phishing, spear phishing and baiting, to induce someone to "open the door" to an attacker. Readily available hacking tools and facilities (e.g. nmap, Netsparker etc) make their job even easier.

2. Use a VPN

Working from home is the new normal now. Using home wi-fi to access university accounts creates opportunity for the cyber criminals.

Few people change their home router password from the factory default password. This means it's easier to hack into home wi-fi networks.

To avoid such incidents, it is always better to use virtual private networks (VPN). The VPN uses "virtual" secured connections routed through the internet from the organisation's private network or a third-party VPN service to the remote site or person.

Most universities, if not all, have the option of using a VPN. It's a highly recommended safeguard against cyber attacks.

3. Get training in cyber hygiene

Academics deal with such sensitive and, for the criminal, exquisite data and resources that they should complete courses (micro-credentials) on cyber-safe teaching or cyber hygiene. This should be required to be compliant for teaching in the digital era.

Yet, currently, there are no such mandatory short courses on cyber hygiene for academic staff.

Read more:* *Universities are a juicy prize for cyber criminals. Here are 5 ways to improve their defences

---

Costs of security breaches can be huge

The sensitive credentials of students and staff that hackers can obtain include names, residential addresses, dates of birth, phone numbers, email addresses, emergency contact details, tax file numbers, banking details and other payroll information. Hackers can use any combination of these details to launch successful social engineering attacks that manipulate the victims. And it's not only the initial victims; cyber criminals also target victims' friends and families.

#privacy #security #CyberAware #network #internet
#technology #tech #technews

5:06 PM · Oct 22, 2020

6 See the latest COVID-19 information on Twitter

If learning management systems are compromised, that can lead to multiple worst-case scenarios. One example is tampering with grades recorded on the LMS. Cyber criminals are offering such services on the dark web and there are plenty of websites selling assignments.

Read more:* *How Australian universities can get better at cyber security

---

Neglecting the cyber security of online platforms used by hundreds of thousands of students and academics across Australia presents an open invitation to cyber criminals. Cyber criminals find the lack of concern for cyber security in the education sector highly alluring.

And hackers can make a lot of money from successful ransomware attacks on students' and academics' computers.

Some universities have paid ransoms to regain access to their data after cyber attacks.

Academic staff might feel they have no option but to pay the ransom to avoid all the legal and privacy-related issues. Students will do anything to regain access to their computer where they probably have stored countless hours of work.

To avoid being put in this position, it is essential for academics and students to complete courses in cyber hygiene. Such courses and regular compliance checks should be mandatory. It is better to be safe than sorry!

Hacking **Online security** **Universities** **Higher education** **Cybersecurity** **Cybercrime** **Internet security** **Cyberattacks** **Cyber defence** **Cyber threats**