Scholars beware: phishing fraudsters hunt for university credentials

Wednesday, 24th October 2018; Kaspersky Lab urges academics to be careful online: the company's researchers have detected multiple cyberattacks hitting at least 131 universities in 16 countries, including South Africa, where several well-known universities have experienced at least one phishing attack in the past year. These attempts to steal sensitive university information have happened in the last 12 months, with nearly 1000 phishing attacks since September 2017. Fraudsters are hunting for credentials of employees and students, their IP addresses and location data. In most cases, they create a web page for entering login and password to universities digital systems, visibly identical to the authentic one.

While the importance of bank employees' credentials or passwords of workers in industrial enterprises is obvious, personal accounts of students and staff at universities might seem to be insignificant targets for cybercriminals. As a matter of fact, the information that could be found through a successful spear phishing attacks on universities might be even more valuable: their databases containing many impactful and exclusive types of research on various topics, from economy to nuclear physics. Besides, since many of them collaborate with leading vendors for PhDs, threat actors might access data containing not only unique expertise but also private and potentially compromising information on companies.

Even though universities are attentive to their IT security, attackers find ways to breach theirs systems by targeting the weakest link– inattentive users. In most scenarios threat actors created a web-page that appeared to be identical to the website of the university, yet differed from it with a few letters in the web address. Usually, victims are quite likely to fall into the trap and enter their credentials sending their sensitive information to phishers, especially if proper social engineering methods are used.

All in all, researchers detected 961 attacks, on 131 schools, aiming mostly at English-speaking universities. 83 of targeted institutions are located in the USA and 21 are based in the UK. The threat actors were especially interested in the University of Washington: Kaspersky Lab detected 111 attacks aimed at this particular school. The statistics show that educational institutions in Asia, Europe and Africa faced attacks too.
"The number of targeted entities is certainly worrying – apparently, the education is becoming a hot topic among the cybercriminals. University staff need to consider that each of their employees and students can become a weak link and provide criminals with access to their systems and be proactive in taking necessary security measures," says Nadezhda Demidova, security researcher at Kaspersky Lab.

Kaspersky Lab recommends taking the following security measure to protect yourself from falling into a phishers' trap:

- Always check the link address and the sender's email to find out if they are genuine before clicking anything – even better, do not click the link, but type it into the browser's address line instead. If you are not sure that the website/ sender is real and safe, never enter your credentials. If you think that you could probably have entered your login and password on a fake page, immediately change your password.
- Never use the same password for several websites or services, because if one is stolen, all your accounts are under risk. To create strong hack proof passwords without having to face the struggle of remembering them, use password managers, such as Kaspersky Password Manager.
- To ensure that no one penetrates your connection to invisibly replace genuine websites with fake ones or intercept your web traffic, always use a secure connection – only use secure Wi-Fi with strong encryption and password, or apply VPN solutions that encrypt the traffic. For example, Kaspersky Secure Connection will switch on encryption automatically, when the connection is not secure enough.
- When using your own device for web surfing, even on a mobile device, always use a robust

security solution that will warn you if you are trying to visit a phishing web page.

- Organisations should educate their employees to never share sensitive data, such as logins and passwords, with a third party and not to click links from unknown senders or in suspicious emails.
- Organisations also should implement a reliable endpoint security solution with anti-phishing technologies, such as Kaspersky Endpoint Security for Business to detect and block spam and phishing attacks.