By ONDREJ KREHEL

Cybercrime is on the rise

Cybercrime is on the rise and journalists are not immune to this trend as they investigate and handle highly sensitive information. They are considered a soft target by cybercriminals since most of them are not concerned or aware that they should secure their information, devices and networks. By lacking user awareness and not practicing proper cyber hygiene, journalists, too, are exposed to many cyber risks such as ransomware attacks, phishing scams, and extortion.

The use of unsecure websites and networks leaves journalists' work vulnerable to the possibility of a cyberattack as they provide a large attack surface. Public networks such as the Wi-Fi in a coffee shop, puts users' data and devices at risk to cyberattack since most public Wi-Fi does not have any level of security. Cybercriminals can exploit network vulnerabilities through man-in-the- middle attacks. These man-in-the-middle attacks are used to access important information such as passwords, usernames, browsing history, and snoop on unencrypted messages sent over the unsecure networks. While public Wi-Fi is one area of risk journalists should be aware of, this also holds true of networks in their own work environment. Journalists should ensure that the networks in the workplace are secured by knowledgeable and trained network administration personnel and that security is up-to-date with the latest anti-virus protection.

Journalists and advertising sales people tend to mine the internet to find leads, following any links that are likely to provide or lead to information that may provide value. This often lands them into traps laid by cybercriminals such as phishing attacks, which are carried out through fake emails, LinkedIn, and other social media accounts. These types of emails contain links that may lead to sites where malware can be downloaded into the journalist's computer. Fake social media accounts use social engineering techniques to coerce users to download and install the malware into their devices. This type of malware can steal confidential information from the journalists' devices and other devices on the network. The malware can encrypt the files and data on the devices making them inaccessible. To access the device and the files, the attackers then demand ransom from the journalist or media company, which may in turn cost the journalist his/her job. This virus can also destroy files and documents stored on the network. Investigative journalists are the most prevalent to this type of cyberattack.

Journalists should be aware of the potential cyberattacks and how they are most likely to take place. They should take initiative in knowing what kind of cyber-weaponry or spyware the hackers are using and how they work. This education will limit exposure to attacks and help in spotting these threats.

Some recommended tips for protecting yourself:

- Avoid the use of public networks, such as hotel Wi-Fi
- Implement virtual private networks (VPN) to avoid interception and spying of communication over the internet.
- Use instant messaging applications that encrypt the messages
- When searching the internet, use secure browsers which do not allow tracking by third parties
- Avoid having the same usernames and passwords for login credentials
- Passwords should be intricate and changed often
- Update software regularly and back up all important information

In case the journalists have been compromised, they should not rush to giving into the hackers' demands. Instead, they should notify their network administrators. Network administrators should contact incident response professionals, such as LIFARS that specialize in identifying, tracking and remediating cyberattacks.

— Ondrej Krehel, CEO and Founder of LIFARS