Cyber Security Awareness

The School of Science and Technology at The University of Fiji, as part of its on-going seminar series, held a Cyber Security Awareness Seminar to mark the Cyber Security Awareness Month on the theme "Do Your Part. #Be Cyber Smart" on October 15, 2020.

Speaking to UniFiji staff and students at the seminar, Mr. Mohammed Farik, Lecturer at UniFiji, emphasized that with the increase in Internet activities by individuals and organisations globally today, there was a greater need for awareness on cybersecurity.

"The three main goals of cybersecurity are to protect data and objects against disclosure attacks which impact the confidentiality of data; to protect data against alteration attacks which impact the integrity of data, and to protect systems and resources against denial of service attacks which affect the availability of data," he stated.

Mr. Farik further explained the top five security threats –*Malware* (software specifically designed to gain access to devices and cause damage; *Web-based attacks* (redirection of web browsers to malicious websites); *Web application/injection attacks* (feeding vulnerable servers and/or mobile apps with malicious inputs with the objective of injecting malicious code); and *DDoS* (Distributed Denial of Service) targets businesses and organizations by making systems or networks unavailable to its intended users).

The focus of this seminar was on Phishing attacks. Phishing attacks attempt to steal or intercept user names, passwords, and financial credentials by combining spoofed emails and counterfeited websites.

"There are three types of phishing attacks: mass-scale phishing is where the fraudsters cast a wide net attack, spear phishing is tailored to a specific victim or a member of a department, and whaling targets the biggest fish – the CEO of a company," he said.

According to Mr. Farik, maintaining good digital hygiene is essential in successfully defending against all types of attacks. This includes defenses such as using : Endpoint devices (laptop or smartphone) that are built to support cybersecurity; vendor-supported operating system software versions; privacy and security capable web browsers; email client software that have spam filter; multifactor authentications; and a premium quality Antivirus software.

He said that the best defense against phishing attacks is the users themselves. It's the user's ability to be able to recognize a phishing email, phishing website, or a phishing hyperlink, and decide smartly whether or not to click.

He informed the participants to watch out for phishing traits such as emails from unknown sources, links with incorrect domain names, errors in grammar and typos, unnecessary file attachments, and motivation factors such as urgency, authority, fear, scarcity, and social proof.

"Stop and think before clicking any links or attachments. If things look 'phishy', verify with the authentic sender through a different medium. When in doubt, throw it out, you are the last line of defense," he said.

Cyber Security Awareness Month was launched by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security in October 2004 and is since celebrated internationally.