Editorial

The Weakest Link in Cyber Security

Kaukab Jamal Zuberi

An organization can have the best IT security in the world but without user awareness about cyber threats and their safe behaviour, it can ultimately lead to failure. End users or "humans" are the weakest link in the security chain at any level. To further strengthen the cause of better end user awareness, research conducted by the University of Toronto which showed clearly that increased user awareness decreases the risk of cyber-attacks.

A cyber-attack is an event in which one or more persons gain unauthorized access to information systems. It can result in information damage, data theft, hardware theft, and temporary or permanent closure of the victim's operations. Reported statistics show that only small part of the victims is able to detect the attack and significantly less people take necessary actions to counteract it.

Cyberattacks can be one of the biggest threats to any business, no matter how small or large. While businesses need to protect themselves from potential cyber attacks by investing in the right security measures, another important factor to consider is ensuring that the members of staff are aware about the issues of cybersecurity and adhering to security protocols. Otherwise, chances are there that vulnerabilities will remain within an organization and it is definitely something which should not be overlooked.

Every time we open our web browsers we take risks, but some websites ask too much. At first sight it may seem just a small issue but it holds a serious risk for the users' systems.

Cybercriminals are now targeting employees on a larger scale and the damage due to corporate espionage has seen a steady increase. Recent reports say that cyber attacks via the supply chain are also increasing, where malicious code is hidden in hardware or software with the help of insiders. This means that end users are becoming increasingly important targets for cybercrime groups. The latest Symantec Internet Security Threat report shows that malicious actors have started to focus on these employees who handle critical business data and sensitive information. Cybercriminals use different methods to subvert them. For instance, they send fake emails claiming to be from the CEO's office asking for money transfers or login credentials or steal sensitive data on USB flash drives dropped into the company mailboxes.

Protecting your network is hard and is one of the major reasons why companies can't effectively protect their own networks is because

they don't have enough supporting technologies in place to do so. Cyber attackers are too sophisticated, even for most large cloud providers, so relying on vendors alone to prevent cyber attacks can be a big mistake. Therefore, it's important to fully understand what you're up against and what you can do to prevent attacks from striking your infrastructure in the first place. But achieving this goal is easier said than done...

There has been a lot in the news recently about computer programmers, IT consultants (both from U.S. and abroad) and I.T. specialists being placed on H-1B temporary work visas or permanent residencies by American companies so they can meet increased demand for their services. This has been dubbed the "brain drain" as these are positions that could be filled by U.S. citizens if not for a lack of interest in the field of computers and information technology, the high cost of education for these fields, and the fact that skilled individuals are outsourced from their home country for MUCH less than an American citizen would make, if not paid as an illegal alien (a common practice).

We have all heard the news about cyber attacks on organizations and individuals with the intention of stealing money, or personal information. The goal is to collect all the data on one system so that they can make money off of it. Over a period of time, monitoring cyber threats has become very important. The weakest link in a chain is the most vulnerable to breakage and the same applies to organizations which are susceptible to cyber attacks when it comes to user behaviour. Users are the weakest link in cyber security and hence proper training on email security should be at priority for anyone who uses email regularly even if you don't believe your employees can fall prey to such attacks.

The increasing need to raise awareness for creating cyber security awareness among the end users has led people to ignore this as an aspect that does not concern them. The cons of this attitude have made their way to the fore in a big way because of increased cyber attacks in the world.

According to reports published by government cyber authorities, over 80 percent of cyber attacks worldwide are attributed to the negligence of system administrators, with users being the weakest link in terms of cybersecurity. Unfortunately, in Pakistan, there is a significant lack of awareness among end users, posing a considerable risk to vital institutions and commercial organizations that form part of the critical infrastructure. To address this issue, the government should implement impactful strategies, policies, and incentives to enhance user awareness in both the public and private sectors. By doing so, the country's critical infrastructure can be effectively safeguarded.