Institute of Engineering & Management

Free iPad Scam

Facebook and Twitter users are complaining about their accounts being compromised and then being used to spam friends with suspicious free iPad offers. Twitter warned users of the scam, saying, "If you received a message promising you a new iPad, not only is there no iPad, but also your friends have been hacked."

The scam is also hitting Facebook users, according to the company's spokesman. "It's affecting an extremely small percentage of people on Facebook, but we take these threats seriously," Simon Axten said via email.

Online marketing programs pay cash for Web traffic, and hackers have found that by phishing victims and then using that information to break into legitimate Twitter and Facebook accounts, they can earn money. The spam is particularly effective because the message appears to come from a trusted source.

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091

Institute of Engineering & Management

IEM's white hats Wi-Fi hacking shows vulnerability of business data

IEM white hat hackers have shown that usernames, passwords, contact lists, details of e-commerce accounts and banking details can be sniffed easily from public Wi-Fi hotspots. To illustrate one of the many ways people can have their data compromised, the IEM hackers conducted two tests in partnership with security firm.

Digitally signed malware a fast-growing threat, say IEM researchers

Digitally signed malware is a fast-growing threat that is aimed at bypassing whitelisting and sandboxing security controls, say security researchers. This is malware that is signed using legitimate digital certificates that have not been stolen or forged, but acquired from certificate authorities or their sub-contractors.

Digitally signed malware a fast-growing threat, say IEM researchers

Digitally signed malware is a fast-growing threat that is aimed at bypassing whitelisting and sandboxing security controls, say security researchers. This is malware that is signed using legitimate digital certificates that have not been stolen or forged, but acquired from certificate authorities or their sub-contractors.

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091

Institute of Engineering & Management

Security incident response below par at most firms

Most firms are not as prepared as they should be for responding to cyber-attacks. But with sensible reviews of processes and communications strategies, up to 70% of firms could put themselves on a much better footing. Early detection of malicious activity is a top priority to defend against cyber attacks by highly motivated threat actors.

Businesses urgently need to reduce the time it takes to detect malicious activity on their networks, according to IEM IT Security Department. The report identifies early detection as a top priority to defend against sophisticated cyber attacks by highly motivated threat actors.

New risks associated with Adobe Flash, the evolution of ransomware and the Dridex mutating malware campaign reinforce the need for reduced time to detection.

Exploits of Adobe Flash vulnerabilities – which are integrated into the Angler and Nuclear exploit kits – are on the rise, the report said, due to the lack of automated or regular patching.

The creators of quickly mutating Dridex campaigns have a sophisticated understanding of evading security measures, the report said. As part of their evasion tactics, attackers rapidly change the emails' content, user agents, attachments or referrers, and launch new campaigns – forcing traditional antivirus systems to detect them anew.

IEM security researchers found the types of common threats that will challenge organisations as the digital economy and the internet of things create different attack vectors and revenue opportunities for cyber attackers.

Angler is one of the most sophisticated and widely used exploit kits because of its innovative use of Flash, Java, Internet Explorer and Silverlight vulnerabilities. It excels at evading detection by employing techniques such as domain shadowing, where stolen domain account credentials are used to create subdomains directed at malicious servers, giving the attacker a huge number of web addresses to cycle through and discard after use

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091

Institute of Engineering & Management

Cyber risk gathers pace

IEM security researchers found ransomware remains highly lucrative for hackers, as the criminals continue to release new variants. Ransomware operations have matured to the point that they are completely automated and carried out through the dark web. To conceal payment transactions from law enforcement, ransoms are paid in crypto currencies, such as bitcoin. The innovation race between adversaries and security suppliers is accelerating placing users and organisations at increasing risk. Suppliers must be vigilant in developing integrated security systems that help organisations be proactive and align the right people, processes and technology. IEM is aiming to take the lead in this direction in response to the fact that business strategy and security strategy are the top two issues for many organisations.

Staying safe on Social Networking sites

- **Limit the amount of personal information you post**
- **Remember that the Internet is a public resource**
- **Be wary of strangers**
- **Be skeptical**
- **Evaluate your settings**
- **Be wary of third-party applications**
- **Use strong passwords**
- **Check privacy policies**
- **Keep software, particularly your web browser, up to date**
- **Use and maintain anti-virus software**

Y-12, Block -EP, Sector-V
Salt Lake Electronics Complex, Kolkata - 700 091