IT SECURITY NEWSLETTER

Issue No.1298/IT – August 2016

Security Tips

1. Be physically aware of your laptop and mobile devices at all times.
2. Ensure your computer has whole disk encryption.
3. Have your screensaver set to auto lock based on inactivity.
4. Don’t accept promotional usb sticks.
5. Use a laptop privacy filter on your screen.
6. Pay special attention to social engineering activities in social media, blogs and emails.

TRA warns against mobile games requesting geographical locations

The UAE Telecommunications Regulatory Authority (TRA) has called on all smart mobile and device users and warned them about playing online electronic games that request for their geographical locations, which could be used against them for criminal activities.

The warning was issued in the light of the growing popularity of online games, especially Pokemon Go, which invades the privacy of users and allowing criminal elements like hackers to spy on them and know when they are in isolated places--giving them the opportunity to rob them of their possessions or cause further harm.

TAQNIA Cyber, Koeing Solutions open cyber academy in Riyadh

TAQNIA Cyber, an information security company in the Kingdom of Saudi Arabia and IT training provider Koeing Solutions, have partnered to open a cyber-academy inside Riyadh's Business Gate. The academy is expected to develop and offer advanced IT programs and highly technical cyber security training programs for IT professionals in Saudi Arabia and surrounding countries.

According to TAQNIA Cyber officials, the academy will cater to the needs of cyber security experts from leading banks, financial institutions, government entities, law firms, healthcare centres, and utility and transportation providers. The academy will prepare security professionals such as penetration testers and network security administrators to use advanced hacking techniques and to learn how to identify and prevent threats before they impact their organization.

Qatari bank gets nod for ‘finger vein pattern’ ATM technology

Qatar's Commercial Bank has announced that it has obtained approval to introduce new finger vein pattern recognition technology to its ATMs, allowing customers to withdraw cash without the need for a bank card or PIN number. The technology will also be extended to corporate and VIP customers to access their Internet banking accounts using a finger vein scanner.

The technology maps the internal vein system within a finger, and will only accept a living finger unlike fingerprint scanning, meaning that authentication requires the customer to be present in person each and every time.

Hackers outwit online banking identity security systems

Criminal hackers have found a way round the latest generation of online banking security devices given out by banks. After logging in to the bank's real site, account holders are being tricked by the offer of training in a new "upgraded security system". Money is then moved out of the account but this is hidden from the user. Experts say customers should follow banks' official advice, use up-to-date anti-virus software and be vigilant.

Devices like PINSentry from Barclays and SecureKey from HSBC - which look a lot like calculators - ask users to insert a card or a code to create a unique key at each login, valid for around 30 seconds that cannot be used again. This brought a new level of online banking security against password theft.

Bahrain set to become a cyber-security hub

Bahrain is set to become a hub for cyber technologies and security after the Kingdom was chosen to become a ‘Centre of Excellence’ by a team of experts from London-based Vauban Group. With the implementation of the project, around 23 companies specialized in various aspects of cyber technologies and security will bring their expertise to Bahrain.

The group aims to serve midsize companies who cannot afford to buy the technologies that are needed to protect their digital assets.

Michael Phelps Targeted by Hackers After Winning 19th Gold Medal

Just a few hours after Michael Phelps added a 19th gold medal, the hacker group ‘New World Hackers’ has compromised his website, just after he took home an Olympic gold medal in the 4x100-meter relay in Rio de Janeiro. New World has made a name for itself by attacking celebrities and other high-profile targets. Previous targets have included GOP presidential nominee Donald Trump, the singer Adele, the BBC and government websites in Pakistan.

The group claims to be carrying out the attacks in the name of "security research," saying that the victims should "take this as a guide, how to secure a site, accounts and more."

For more information, enquiries and events please do not hesitate to contact us:

Ranjith Kumar, Director, *ranjith.kumar@keypoint.me*, +973 17206 827

Chahira Ashcroft, Senior Manager, *chahira.ashcroft@keypoint.me*, +973 17206 870