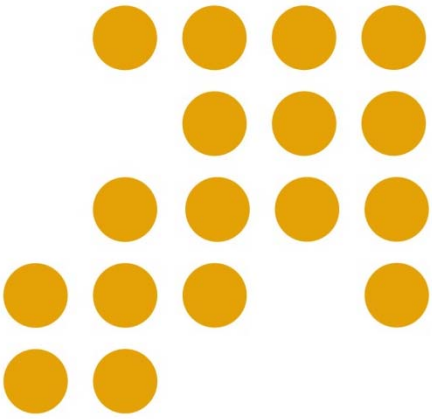
Cyber Security Policy Research Division

CYBER SECURITY INCIDENT OUTSIDE MALAYSIA

Report No. 12 – August 2010

16 August 2010



CyberSecurity Malaysia

Level 8, Block A,

Mines Waterfront Business Park

No 3, Jalan Tasik

The Mines Resort City

43300 Seri Kembangan

Selangor Darul Ehsan

Securing Our Cyberspace

An agency under

MOSTI
Ministry of Science, Technology and Innovation

TABLE OF CONTENTS

1 FRAUD

1.1 FAKE DISLIKE BUTTON FACEBOOK SCAM

Facebook users should be wary of the latest survey scam spreading virally across the network. There are a number of variations of this scam, which sees users unwillingly update their Facebook status encouraging others to get the "official dislike button". The scam is spreading quickly as many Facebook users have been calling for the introduction of an official "dislike" feature which would allow them to express their opinions on other users' posts, links and updates. Two versions of the scam have been discovered by Sophos, which involve the sharing of messages with the text: "I just got the dislike button, so now I can dislike all of your dumb posts lol!! LINK" and "Get the official DISLIKE button NOW! LINK". The viral scam, similar to many recent survey scams, tricks users into giving a rogue Facebook applications permission to access their profile, silently posting and promoting the link that tricked the user in the first place and spreading the message virally. At this stage, the user still does not have access to the "Dislike" feature and the application finally asks them to complete an online survey which makes money for the scammers.

Source: Help Net Security, 16 August 2010
http://www.net-security.org/secworld.php?id=9740

1.2 CLICKJACKING THREAT PUNTS FACEBOOK SURVEY SCAM

The latest assault relies on tricking users into using the Facebook "Share" feature without notifying surfers that content is being shared. By contrast, an otherwise similar clickjacking attack dating back from May relied on duping a user into injudicious use of the social network's "Like" feature. Sophos explains that the opening move for the latest attack poses as a "Facebook fan page" for the “Top 10 Funny T-shirt Fails ROFL” and other potentially eye-catching content. These fan pages, once selected; load malicious script from an external domain that means the user will unwittingly share the dodgy page on their profile, promoting the scam to friends and contacts on Facebook.

Source: The Register, 18 August 2010
http://www.theregister.co.uk/2010/08/18/facebook_clickjacking_scam/

1.3 JUSTIN BIEBER OFFERING FREE TICKETS ON FACEBOOK? IT'S A SCAM

Bieber fans have been targeted by the latest Facebook scam - agree to let the application post messages on your wall and subscribe for a £4.50 per week premium rate service, and you will get free tickets to a concert of the young star. According to Sophos, the scam is spreading virally, thanks to Bieber's immense popularity and the users' propensity to trust their "friends" recommendations. This is not the first time that Bieber's name was used by cybercriminals, and he is definitely not the only celebrity whose fame is being misused.

Source: The Help Net Security, 19 August 2010
http://www.net-security.org/secworld.php?id=9762

1.4 MESSING WITH INTERNET SCAMMERS

Online scammers are resourceful people who take advantage of people's gullibility and lack of knowledge about Internet dynamics, but once in a while they happen to stumble upon users who will know who they are dealing with and are willing to play along and lead them on a merry chase. Trend Micro researcher David Sancho is one of those. Admittedly, it's his job to do so, but it is nevertheless very nice to see an intended victim waste the spammers' time.

He caught the fraudster's attention by putting up an advertisement on Facebook Marketplace, in which he professes his intention of selling his car. A few hours pass, and he is contacted by a woman named Caroline McMillan. She asks for further details, agrees on the price without even seeing the car and says she will be paying through PayPal. Immediately, Sancho gets suspicious, why would anyone buy a car without seeing it first? And paying through PayPal? He does a quick online search, finds accounts of similar scams that convince him that he's talking to a scammer, and decides to have some fun and discover all he can about it.

Source: Help Net Security, 20 August 2010
http://www.net-security.org/secworld.php?id=9766

1.5 FACEBOOK SCAM: "I MAY NEVER TEXT AGAIN AFTER READING THIS"

Sophos is warning Facebook users about a new scam that is spreading quickly across the social network claiming to be a link to an article, "I may never text again after reading this". Despite similar scams over the past month, including one involving a fake "Dislike" button, over 200,000 Facebook users have already "liked" the rogue page. Not only does this help the scammers to earn money, but it also means that at any time the unknown owner of the page can send users an update which could contain an unwanted advertising message or a malicious link. Facebook users that have been affected should delete references to this scam from their wall, to avoid sharing it further with their online friends.

Source: Help Net Security, 24 August 2010
http://www.net-security.org/secworld.php?id=9778

1.6 ITUNES/PAYPAL SCAM IS DUE TO PHISHING, NOT A BUG?

A recent flurry of iTunes customers' reports that their accounts must have been hacked and used to execute purchases via PayPal that occasionally total up to thousands of dollars, has raised the question of whether Apple's App Store has again suffered a breach. But, as it turns out, Apple is not to blame in this case. The company claims that there is no security hole in iTunes, and that the users in question must have fallen for a phishing scam. According to Charles Arthur, some of the victims insist that they have never given out their iTunes or Paypal account credentials before checking that the website requesting them is legitimate. At this time, the theory that these users have been recycling usernames and accounts using the same combination for a number of online services, some of which could have been hacked more easily is more likely one. Apple has recently improved App and iTunes Store security measures, requiring more frequent re-entry of a customer's credit card security code. But, this is obviously not enough the smartest thing to do here would be to remove all automatic payment options. Apple will probably pass on that, but users should consider it.

Source: Help Net Security, 24 August 2010
http://www.net-security.org/secworld.php?id=9789

1.7 U.S. VISITORS EASY PREY FOR ONLINE SCAMMERS

As you may already know, travelers from the 36 countries that don't require a visa to enter the U.S. must still register online for travel authorization. And as of September 8, 2010, they will also be required to pay a $14 fee for it. Since this registration can be performed exclusively online and registrants are largely unfamiliar with official U.S. government sites and registration processes, this requirement is a dream come true for various scammers and other

online criminals. Fake websites offering ESTA (Electronic System for Travel Authorization) forms have been popping up left and right for quite some time, and the announced fee has attracted even more malicious individuals in search for a quick buck. Since the registrants expect to have to enter a variety of personal information in order to get the travel authorization, they are naturally less likely to spot something unusual.

Source: Help Net Security, 25 August 2010
http://www.net-security.org/secworld.php?id=9786

1.8 FAKE SURVEYS HARVEST PERSONAL INFORMATION

Gifts are often used as an incentive to make people share their personal information. Way back in the day, people could be convinced to share their password in return for a chocolate bar. Today, $200 gift certificates and expensive devices are offered. Symantec warns about a spam run that seeks to lure the recipients into completing a bogus survey on features provided by their social networking site. To make the survey seem legitimate and to assure themselves that the information they receive is not bogus, the people behind this scheme make it clear that only participants that are over 18 years of age and are U.S. residents are eligible to receive the gift, and that the provided information must be valid, or the gift will not be delivered to the survey-taker. It is good to remember that sharing any kind of personal or financial information after following a link contained in an unsolicited email message is a really bad idea. At best, your information is now in the hands of Internet marketers that will seek to use it or sell it to others who are interested in spamming you with offers you did not seek. At worst, your information will be used by various criminals to steal your identity, money or get you into debt.

Source: Help Net Security, 30 August 2010
http://www.net-security.org/secworld.php?id=9795

2 HACK THREAT / INTRUSION

2.1 UNDERGROUND CREDIT CARD CLEARING HOUSE HACKED

An investigation by Trend Micro has confirmed, an underground credit card clearing house has itself been hacked. The operation - a holding firm for anonymous payment service Fethard - processes credit card payments for a rogue's gallery of fake anti-virus (scareware) suppliers, spam-promoted unlicensed pharmaceutical and extreme pornography sites. Hackers claimed to have breached a server behind its website on 23 July, publishing information online including employee emails and recorded phone calls, one discussing techniques to defraud credit card firms. The perpetrators of the hack and their motive remain unidentified, but it is potentially an assault from cybercrime rivals. Trend said the information on the unnamed credit card processor, registered in the Netherlands but actually run from Russia and Latvia, checks out. The firm has legitimate customers in Russia as well as rather more unscrupulous clients, reportedly taken on to keep the business afloat after it became the victim of cybercrime itself a few years ago.

Source: The Register, 16 August 2010
http://www.theregister.co.uk/2010/08/16/underground_credit_card_clearing_house_hacked/

2.2 WHO IS THE TYPICAL RUSSIAN HACKER?

Security analyst Fyodor Yarochkin and a senior researcher from security firm Coseinc that calls himself "Le Grugq" have spent 6 months on various Russian web forums in order to discover just what kind of threat Russian hackers present to the world at large. Both of them fluent in the language,

they managed to get more than just a glimpse into this underground culture and shared their knowledge with the attendees of last month's Hack in the Box conference. Enterprises have little to worry about, since Russian hackers are usually attracted by money - but money they can get their hands on simply and fast. Corporate secrets hold appeal to them. They often go for the easiest potential victims, and that is usually the careless individual user. The typical Russian hacker is a student looking for some pocket money. His targets are individual users in the Western world and he has no qualms about fleecing them since he believes everybody is rich outside Russia - claims Yarochkin. Russian hackers are geeks, not gangsters.

Source: Help Net Security, 16 August 2010
http://www.net-security.org/secworld.php?id=9739

2.3 HACKED SMARTPHONES POSE MILITARY THREAT

Hacked smartphones could endanger troops by sending location data to the enemy using mechanisms similar to those employed by recently discovered Android malware. Malicious software that commandeers phone functions could give wartime enemies valuable information about troop locations and movements, according to Hugh Thompson, a software security professor at Columbia University and conference chairman for the RSA Confernece, and Markus Jakobsson, who works on the PayPal online security and malware strategy team. Thompson says, "Even normal apps can send a lot of information back home, and individual users are generally ill equipped to determine whether these apps represent security risks.

Source: Computerworld, 16 August 2010
http://www.computerworld.com/s/article/9180768/Hacked_smartphones_pose_military_threat

2.4 HACKED AXL ROSE TWITTER ACCOUNT SPREADS FALSE TOUR NEWS

Axl Rose's Twitter account was hacked on Sunday to spread false rumours that Guns N' Roses was cancelling an upcoming European tour. It's unclear who actually controls the profile at present, which was likely hacked by a password guessing or perhaps password reset attack. Many other celebs including Britney Spears, Lindsay Lohan, British politician Ed Miliband have previously fallen victim to Twitter hackers.

Source: The Register, 17 August 2010
http://www.theregister.co.uk/2010/08/17/axlrose_twitter_hack/

2.5 APPLE.COM HIT IN LATEST MASS HACK ATTACK

A hack attack that can expose users to malware exploits has infected more than 1 million webpages, at least two of which belong to Apple. The SQL injection attacks bombard the websites of legitimate companies with database commands that attempt to add hidden links that lead to malware exploits. While most of the sites that fell prey appear to belong to mom-and-pop operations, two of the infections hit pages Apple uses to promote iTunes podcasts, this Google search shows. The malicious links appear to have been removed since Google last indexed the pages in early August. In all, at least 538,000 pages have been compromised by the same attack. Attacks that bare similar fingerprints but point to different domains, have claimed close to 500,000 more. “These attacks have been ongoing and are changing pretty often,” said Mary Landesman, a senior researcher with ScanSafe. SQL injection attacks succeed because web applications don't properly filter search queries and other user-supplied input for malicious text. When the data is processed, commands are passed to a website's backend server, causing it to add links or cough up sensitive information.

Source: The Register, 17 August 2010
http://www.theregister.co.uk/2010/08/17/apple_sql_attack/

2.6 IRANIAN ACTIVISTS DEFACE UK GENETICS WEBSITE

The UK's Human Genetics Commission website was hit by politically-motivated hackers on Tuesday, who defaced the site with a protest marking a Western plot to overthrow a post-WWII democratically elected leader in Iran. Dr Mohammed Mossadegh nationalised Iran's petroleum industry before a plot backed by the UK and the US led to his overthrow back in 1953. Quite why the Sun Army defaced the Human Genetics Commission website with digital graffiti is not immediately clear, but Jason Hart - senior European VP of CryptoCard, said that in "order to deface the site they [the hackers] would have had to get admin access". Iran is something of a hotbed for politically-motivated hack attacks. The Iranian Cyber Army mounted a series of DNS hijacking attacks against first Twitter and later Chinese search engine Baidu in December 2009 and January. The attacks both resulted in the redirection of surfers.

Source: The Register, 19 August 2010
http://www.theregister.co.uk/2010/08/19/iran defacers_hit_genetics_website/

2.7 THE DANGERS OF INSIDER THREAT

Whilst the media seems pre-occupied with the problems of cybercriminals causing problems for organizations from outside their network, a survey just published shows that 23 per cent of UK employees will take customer lists and other sensitive data when they leave their employer. According to Amichai Shulman, CTO of Imperva, "more than anything, this highlights something we've been saying for some time, namely with insider threats, IT managers are fighting a less visible, but not less difficult threat in addition to the well publicized external threats. Staffs are precisely the people who have access to data that needs to be secured and carefully controlled." In addition, the survey shows that the insider threat is not always the potentially rogue employee for whom a background check has been completed - staff also need to be monitored during their employment as the information may not necessarily be 'maliciously' downloaded after the termination notice but rather information was rightfully obtained and collected by the employee over time and actually should have been removed upon termination by the IT team.

Source: Help Net Security, 24 August 2010
http://www.net-security.org/secworld.php?id=9774

2.8 DEFCON SURVEY REVEALS VAST SCALE OF CLOUD HACKING

An in-depth survey carried out amongst 100 of those attending this year's DEFCON conference in Las Vegas recently has revealed that an overwhelming 96 percent of the respondents said they believed the cloud would open up more hacking opportunities for them. "While 'only' 12 percent said they hacked cloud systems for financial gain, which still means a sizeable headache for any IT manager planning to migrate their IT resources into the cloud" said Barmak Meftah, CPO with Fortify. In the many predictions, he explained, 20 per cent of organizations would own no appreciable IT assets, but would instead rely on cloud computing resources - the same resources that 45 percent of the DEFCON attendees in the survey cheerfully admitted to already having tried to hack. Breaking down the survey responses, 21 percent believe that SaaS cloud systems are viewed as being the most vulnerable, with 33 percent of the hackers having discovered public DNS vulnerabilities, followed by log files (16 per cent) and

communication profiles (12 per cent) in their cloud travels.

Source: Help Net Security, 24 August 2010
http://www.net-security.org/secworld.php?id=9773

3 PHISHING ATTACK

3.1 COURIER SERVICE CUSTOMERS TARGETED BY PHISHING WEB SITES

Customers of well-known courier services are often targeted by cybercriminals. Sometimes they try to make them open malicious files attached in emails with the excuse of needing them to verify transaction details, but lately Symantec has detected a number of phishing sites that spoof website of courier services. With the pretext that the customer's account hasn't been updated for a considerable time, the site asks the customer to enter account details such as UserID and password, account name and number, and billing address. You might think that this information isn't really that sensitive, but it can definitely be misused by the criminals taking over the identity of the customer with the service in question and - at the minimum - redirect valuable packages to another delivery address. Once the users enter the wanted credentials, they are redirected to the official website of the courier, making the illusion of legitimacy complete. Luckily for potential victims, these phishing websites are not very professionally executed, and certain links lead to error pages.

Source: Help Net Security, 17 August 2010
http://www.net-security.org/secworld.php?id=9743

4 MALWARE

4.1 VIRGIN MEDIA TO WARN MALWARE-INFECTED CUSTOMERS

Virgin Media subscribers whose computers are part of a botnet can expect a letter warning them to tighten up their security, under a new initiative based on data collected by independent malware trackers. The UK's third-largest ISP will match lists of compromised IP addresses collected by the Shadowserver Foundation, among others, to its customer records. Those with infected machines will be encouraged to download free security software to remove the malware and protect their connection in future. Virgin Media says it expects to send out hundreds of letters per week initially, with plans to expand the campaign based on customer feedback.

Source: The Register, 16 August 2010
http://www.theregister.co.uk/2010/08/16/vm_malware/

4.2 MALICIOUS WIDGET HACKED MILLIONS OF WEB SITES

As many as five million Web sites hosted by Network Solutions have been serving up malware, probably for several months. According to Wayne Huang, co-founder and CTO of Santa Clara, "this is one of the biggest infections for drive-by download attacks that I've seen." Network Solutions disputed Huang's estimate of between 500,000 and 5 million infected sites, but was unable to provide its own count. Huang said his firm's researchers initially tracked the infection to a widget installed by Network Solutions on its *GrowSmartBusiness.com* site, then later discovered that the same widget was installed by default on all "parked" domains hosted by the Herndon, Va. hosting giant. Parked domains are those that have been registered, but lack any owner-provided content. Malware makers and scammers

have used these under-construction sites in the past to spread attack code or artificially boost search site rankings to dupe consumers into visiting.

Source: Computerworld, 16 August 2010
http://www.computerworld.com/s/article/9180783/Malicious_widget_hacked_millions_of_Web_sites

4.3 CAMERON DIAZ TOPS MALWARE BAIT LIST

According to McAfee, Cameron Diaz is the most dangerous celebrity on the Web. Search strings using Diaz's name have a one-in-ten chance of coming up with a site infected with or spreading malware. Diaz replaced Jessica Biel, last year's top name bait. Biel fell two spots to third on McAfee's list this year. Actress Julia Roberts placed second on the Most Dangerous list, while supermodel Gisele Buendchen took fourth. Brad Pitt, the highest ranking man on the list and one of only two on the top 10, held the fifth spot. Attackers and scammers trade on the names of prominent people and topical events to dupe users into visiting malicious sites, to open malicious e-mails, and to click on malicious links embedded in Twitter messages.

Source: Computerworld, 20 August 2010
http://www.computerworld.com/s/article/9181158/Cameron_Diaz_tops_malware_bait_list

5 OTHERS

5.1 STOLEN FLASH DRIVE WITH SENSITIVE FINANCIAL INFO

Another example that demonstrates the need to follow security policy when it comes to keeping personal and financial information handled by businesses and organizations secure comes from Portland. Portland's Community College announced that a small flash drive was stolen from the car of an officer of the institution, and that it unfortunately contained sensitive financial information regarding the 2,900 participants of the Oregon Food Stamp Transition Program. As if this wasn't bad enough, the spokesman of the PCC says that the information wasn't password protected or encrypted, and that it would be very easy for the thief to access it and use it. The only mitigating factor here is the fact that the flash drive was in a bag, so it is highly likely that the criminal was after money, not information. According to OPB News, the spokesman says it is definitely against the institution's security policy and protocol to be carrying around this kind of information unprotected, and that situations such as these are precisely the reason why information is kept on various locations, so that employees don't have to transport it.

Source: Help Net Security, 17 August 2010
http://www.net-security.org/secworld.php?id=9749

5.2 7-CHARACTER PASSWORDS SOON TO BE HOPELESSLY INADEQUATE

According scientists from Georgia Tech Research Institute, the increasing processing power and the growing number of processors on graphic cards will soon make 7-character passwords "hopelessly inadequate" to withstand brute force attacks. No combination of alphanumeric characters and symbols will be save users who choose such a short password, because these stream processors work simultaneously in order to process images, and can try out the various combinations of characters and symbols needed to discover a password in a much shorter time than ever before. The researchers advise users to start using 12-character passwords that combine lower and upper case letters, numbers, and symbols. But ultimately, even this will not be enough. CPU power grows every year, and it's only a matter of time until users are forced to pick entire sentences as passwords.

Source: Help Net Security, 17 August 2010
http://www.net-security.org/secworld.php?id=9747

5.3 FACEBOOK LOGIN PAGE STILL LEAKS SENSITIVE INFO

Facebook's login system continues to spill information that can be helpful to phishers, social engineers and other miscreants attempting to scam the more than 500 million active users of the social networking site. When a legitimate email address is entered along with an incorrect password, the authentication system returns an error that reads: "Please re-enter your password. The password you entered is incorrect. Please try again (make sure your caps lock is off)." When an email address that doesn't belong to a Facebook user is entered, the response is: "Incorrect Email. The email you entered does not belong to any account." The difference in the wording makes it possible for anyone to discern whether given emails address is registered on Facebook, even when the corresponding password is unknown.

Source: The Register, 18 August 2010
http://www.theregister.co.uk/2010/08/18/facebook_login_info_leak/

5.4 RESOURCEFUL ATTACKERS CONTINUE TO MAKE THE WEB INSECURE

According to a report by Zscaler, attackers are staying one step ahead of the game and enterprises are struggling to keep up. During the second quarter of 2010, attackers once again took advantage of opportunities just as quickly as they emerged. These opportunities included both the emergence of new vulnerabilities in popular technologies as well as current events that drew the attention of millions around the globe. Q2 included the start of one of the largest global sporting events, the World Cup. It didn't take long for attackers to seize on this opportunity to deliver a variety of World Cup related attacks including poisoning search results with Blackhat SEO techniques and phishing for financial credentials. A new attack trend emerged during the quarter thanks based on the deployment of a new Facebook feature - the Like button – on numerous external sites. Attackers are using likejacking by continually tricking users into clicking like buttons to drive traffic to malicious sites. In certain instances likejacking has been combined with clickjacking to further automate the process.

Source: The Register, 18 August 2010
http://www.net-security.org/secworld.php?id=9755

5.5 EMPLOYEES ADMIT THEY WOULD STEAL DATA WHEN LEAVING A JOB

Employees openly admit they would take company data, including customer data and product plans, when leaving a job, according to Harris Interactive. The online survey probed 1,594 full and part-time employees and contractors in the United States and Great Britain about their attitudes toward accessing and viewing of company-owned data. In response to the survey:

- 49% of US workers and 52% of British workers admitted they would take some form of company property with them when leaving a position
- 29% (US) and 23% (UK) would take customer data, including contact information
- 23% (US) and 22% (UK) would take electronic files
- 15% (US) and 17% (UK) would take product information, including designs and plans

- 13% (US) and 22% (UK) would take small office supplies.

Very few workers (1% in the UK and less than 0.5% in the US) stated that they would attempt to sell confidential data found in improperly secured files, although 2% (US) and 3% (UK) said they would look and tell others about the information they saw.

Source: Help Net Security, 18 August 2010
http://www.net-security.org/secworld.php?id=9754

5.6 SKELETAL SCANNER WOULD ID TERRORISTS FROM 50 METERS

Scientists are developing an identity verification system that would spot terrorists and pedophiles by scanning their skeletal features and comparing them against a database of stored images. The system could be deployed in airports, sporting events, and other settings vulnerable to criminals and ideally will be able to positively identify an individual's unique skeletal structure from 50 meters, the researchers, from Wright State Research Institute. It would analyze a variety of skeletal attributes – including shape, density joint structure and previously broken bones to identify the individual. Using fingerprints to identify someone can be problematic for a variety of reasons, not the least of which is the ease at which a person's unique image can be appropriated by others. Facial recognition has begun to catch on in some places, but that technology can be easily thwarted using masks, beards and other disguises. Of course, the ability to identify individuals from great distances has some spooky implications for privacy. The specter that scanners will be deployed at political demonstrations, outside medical clinics, or similar places will no doubt arouse concern among civil libertarians.

Source: The Register, 24 August 2010
http://www.theregister.co.uk/2010/08/24/skelital_image_scanner/

5.7 TOO MANY DISCLOSE SENSITIVE INFORMATION ON SOCIAL NETWORKS

Social networking users should be careful when accepting friend requests and to be conscious of the data they share. According to a new study by BitDefender, social network users do not appear to be preoccupied with the real identity of the people they meet online or about the details they disclose while chatting with total strangers. The study revealed that 94 percent of those asked to “friend” the test profile, an unknown, attractive young woman, accepted the request without knowing who the requester really was. The study sample group included 2,000 users from all over the world registered on one of the most popular social networks. These users were randomly chosen in order to cover different aspects: sex (1,000 females, 1,000 males), age (the sample ranged from 17 to 65 years with a mean age of 27.3 years), professional affiliation, interests etc. The study showed:

- More than 86 percent of the users who accepted the test-profile’s friend request work in the IT industry, of which 31 percent work in IT Security
- The most frequent reason for accepting the test profile’s friend request was her “lovely face” (53 percent)
- After a half an hour conversation, 10 percent disclosed personal sensitive information, such as: address, phone number, mother’s and father’s name, etc – information usually requested as answers to password recovery questions
- Two hours later, 73 percent siphoned what appears to be

confidential information from their workplace, such as future strategies, plans, as well as unreleased technologies/software.

Source: Help Net Security, 30 August 2010
http://www.net-security.org/secworld.php?id=9793