BESTPRACTICES

CyberSecurity MALAYSIA

KEEP YOURSELF SAFE FROM ONLINE **IDENTITY THEFT**

1.0 INTRODUCTION

Online identity theft is not a new phenomenon to many Internet users. However, today, the Internet has given it a new lease of life. Every minute, thousands of individuals and even companies fall prey to these increasingly sophisticated cybercriminals and attackers. They use various techniques such as social engineering, phishing and devious modus operandi via the Internet targeting potential, innocent victims. They identify vulnerabilities and exploit emails, instant messaging (IM) and the web to trick potential victims into sending them user's credentials and personal information, besides confidential information related to the victims' companies. These information and credentials can be manipulated for many malicious activities on the net and for monetary gains.

One must remember that everyone and anyone is a potential target. These cyber-criminals and attackers often use different tactics to lure different victims. However, the impact is always the same – theft of identities can bring a potential victim immeasurable agony in terms of the credit status, financial status, integrity of a person or to a certain extent, a criminal record.

2.0 HOW DOES ONLINE IDENTITY THEFT WORK?

Online identity theft is different from other types of identity thefts as it will not involve physical stealing of information but rather the victim may unwittingly hand over the information themselves to another party.

Digital identities that represent individuals on the Internet, are made up of information that only the individuals themselves will know about. This can be anything, such as IP (Internet Protocol) address, the mailing address where a person lives, telephone numbers, usernames, passwords, PINs, birth dates, account numbers and the list goes on.

Online applications are often used now due to convenience and its time saving appeal. These applications need a user to key in his/her digital identity in an online form which will be saved in a particular database. If the fraudsters are able to access these digital identities, they can misuse it to commit various fraud activities in the victim's name such as applying for loans or new credit card accounts in the victim's name and then not paying the bills or impersonating victims on social networking websites. These fraudsters or cybercriminals can use the stolen digital identity in intrusions, unauthorised use of cheques or debit cards, or unauthorised electronic transfers from a victim's bank account. They can even sell the stolen personal information in underground economy or post the personal information publicly at online forums. A worst case scenario, fraudsters commit crimes in the victim's name and causes the victim to be answerable to law enforcement agencies and slapped with a criminal record.

There are many ways on how the cybercriminals use devious tricks on victims into providing personal information:

2.1 Phishing

Masquerade behind the realistic appearance

Phishing involves sending out an email that fools the recipient into thinking it comes from a financial institution or other legitimate entity. Duped by the email's realistic appearance, right down to the logo and sender name, plus the false urgency and negative implication for not responding immediately created by the fraudster, the recipient is then directed to a website where they are asked to update or confirm account information (account number, password etc). Sensitive data and unhindered bank account access have been delivered straight into the hands of cybercriminals.

2.2 Pharming

Fake website but real IP address

Pharming works invisibly! The cybercriminals hijacks the domain name server (DNS) of a commercial site and redirect visitor's web requests to a fake site. Essentially, anyone who enters to the genuine web address will be taken to the identical but bogus website. If the appearance of the fake website looks exactly the same as the genuine site, the victim will enter his/her personal information without thinking twice.

2.3 Spyware

Lurks behind seemingly innocent websites

Online Identity theft can also happen when a person did not realize downloading the spyware. Spyware is hardly noticeable as it is usually bundled together with other freewares such as screen savers, image editing tools, smiley icons, etc. It can also be downloaded when the person is tricked into downloading a dangerous email attachment or when he/she visits a website that is infected with malicious codes. The programme then collects personal information, such as credit card numbers and bank account numbers. This information will be sent to cybercriminals who uses it to steal a person's identity.

2.4 Social Networking Profiles

Once data is put online, it is impossible to be totally removed

Social networking sites have become hot spots for cybercriminals to commit identity theft. The users may not realize how much information they provide to identity thieves unknowingly through their social networking profiles. Seemingly harmless personal information concerning their full names, partners, pets, mother's name, schools they went to or birth dates, provide excellent clues for cybercriminals to figure out their passwords. Even sharing their experience on using online banking, gives cybercriminals information on the types of banking users indulge in or types of accounts users have. When all these pieces of seemingly harmless information are put together, cybercriminals are able to use social engineering tactics or phishing to steal identities.

3.0 HOW TO PROTECT FROM ONLINE IDENTITY THEFT

By eliminating the vulnerabilities and being vigilant about protecting personal information, you can reduce the risks and dangers of being a victim to identity theft.

3.1 Install anti-virus and anti-spyware software and keep them updated with the latest security patches

Viruses and spywares have become sophisticated in the hand of cybercriminals that they are able to infiltrate computer systems and steal data. Having proper updated version of antivirus and antispyware is not enough; you must also ensure your computer is updated regularly with the necessary latest security patches. You can refer to the respective vendors' websites for the latest security patches.

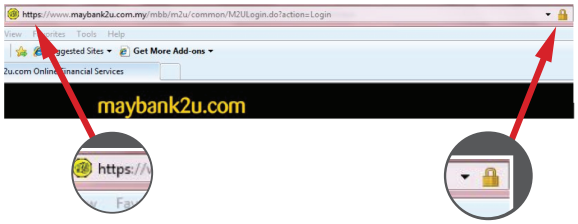
3.2 Limit the information posted on the Internet

Be stingy in revealing amount of personal information on the Internet such as your full name, birth date, address or credit card number. The same goes when shopping online and the site requires you to provide certain information to process your order. Do not give information more than is required to process your order such as leisure lifestyle or your annual income. If this information falls into wrong hands, it will make identity theft extremely easy.

3.3 Conduct online transactions only at secure websites

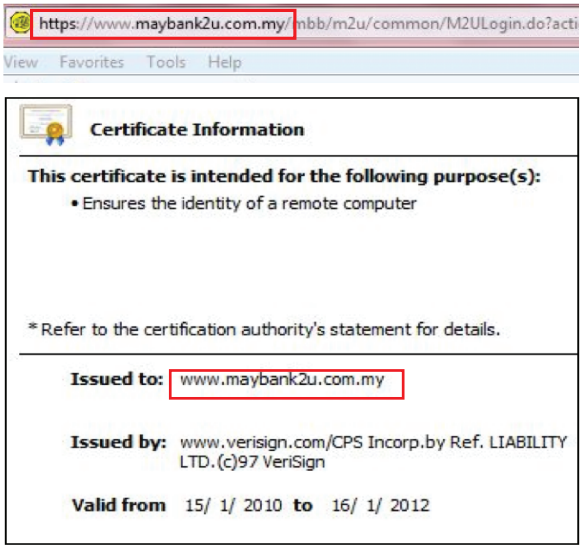
Any websites that requires you to provide login credentials, personal identifying information or financial information should provide Secure Socket Layer (SSL) authentication. SSL provides a security mechanism such as digital certificates and encrypts all transactions between your computer and remote websites to prevent data being read by hackers.

Make sure these websites implement correct SSL procedures by checking the correct form of the SSL website address (using 'https ://...') and the presence of a closed padlock icon as shown in the picture below.



3.4 Don't be fooled by spoofed website

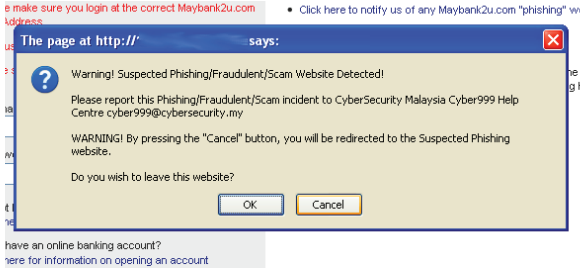
It is vital to do further checking on the websites' digital certificate. Although these websites are using 'https://…' address and has a closed padlock icon, there is still a possibility that it may not be secure. Several phishers design spoofed websites that happen to have those padlock icons. Double-check the digital certificate by clicking on the closed padlock icon. Look at the "Issued to" in the pop-up window and you should see the name matches with the website that you are on as shown in the picture below.



Leave the websites if you find the name differs from the genuine ones.

3.5 Install DontPhishMe

For the Mozilla Firefox user, use DontPhishMe to alert you if an online banking web page that you visit appears to be asking for your personal or financial information under false pretences. DontPhishMe will automatically warn you as shown in the picture below, when you encounter a page that is trying to trick you into disclosing personal information.



DontPhishMe is an initiative of MyCERT, CyberSecurity Malaysia, to provide a security mechanism in preventing online banking phishing threat specifically for local Malaysian banks. You can download and install DontPhishMe from Mozilla Firefox add-ons' repository.

3.6 Implement a strong password and keep it safe

When creating a password for online transaction, make sure you use a good, strong password. One way of creating a good, strong password is using a phrase with combination of alphabets, numbers, uppercase letters, lowercase letters and symbols. Get a phrase that you can remember and take the first letter of each word as your password, then convert to the letters that you can remember. For example, “I love study at Mc Donald” would become “I<3starD@McD”. The password should be long enough e.g. eight (8) characters or more. Never share your password with others and change the password on regular basis, preferably, every 6 months.

3.7 Know who you invite into online network

Posting information on social networking is like broadcasting it on commercial TV. Therefore, you should restrict who can access your profiles and do not accept into your network strangers or unknown persons as they could be phishers. You need to check and refer to the security settings provided by the respective social networking sites.

3.8 Read the web site’s privacy policy

Read the privacy policy of websites (especially social networking sites) prior to submitting confidential and personal data. Learn what type of information they gather in their sites and check if they allow the third parties to access to your information without your prior permission. Be extra cautious with the companies that make frequent changes to their privacy policy.

3.9 Be careful with what you download or when opening email attachments

Think twice before downloading a “free” game or gadget from unknown sources or opening an email attachment from someone that you do not know. These downloaded files or attached files may contain malicious codes to steal your personal information. Do so only when your trusted anti-virus programme is running. Always scan the downloaded items or files with an updated version of your anti-virus software before running or executing them in your computer.

You can also download a reliable online virus and URL scanner from internet that analyses suspicious files and URLs for viruses, worms, trojans, and all kinds of malware that can be detected by anti-virus programme.

3.10 Be wary with wireless network

Having an unsecured wireless network such as unprotected Wi-Fi allows anyone within range of your location to access your network or ride on your Internet connection. Be extra careful when using a wireless networks to read your emails or while doing online banking as you are susceptible to identity theft since cybercriminals who may be lurking in the neighborhood can “see” what you do online.

You should not connect to a wireless network without encryption enabled or Wireless Encryption Protocol (WEP) enabled. You must always connect to an access point with a strong encryption protocol in place such as Wi-Fi Protected Access (WPA or WPA2) with mutual authentication 802.1 x protocols.

For Mozilla Firefox users, you can use HTTPS Everywhere or Force-TLS, a Firefox security add-on, that force the Firefox browser to establish HTTPS (secure) connection to websites you visit by changing the HTTP to HTTPS; provided that those websites support HTTPS. These Firefox add-ons protect the login information and ensure a secure connection is established to majority of websites. You can visit Mozilla Firefox’s website to download the add-ons.

3.11 Get your browser updated

The common problem that causes users fall victim into identity theft is the use of outdated browsers. Make sure to have your browser upgrade to e.g. IE7, Firefox 3.0 or Opera 9.5 or higher as these browsers have anti-fraud tools in place to protect your personal and financial information. You can refer to the respective vendor’s website for latest browser updates.

4.0
WHAT DO YOU NEED TO DO IF YOU SUSPECT YOUR IDENTITY HAS BEEN STOLEN

- If the stolen identity involves financial or credit card information, report immediately to your banks or credit card companies for them to initiate the necessary remedial action.
- Lodge a police report immediately at a nearby police station with supporting documents.
- Change the password immediately if your identity has been stolen due to account compromised. Get assistance from your service provider if you have difficulty retrieving back your password.
- Report to your local Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) for assistance on identity theft incidents.
- Contact Cyber999 to report incidents related to identity theft.

5.0
MORE TIPS ON SECURITY

In order to get other tips on how to protect yourself and your computer, please visit our website at http://www.CyberSAFE.my

6.0
REFERENCES

- http://onlineidentitytheft.org/
- http://www.guard-privacy-and-online-security.com/internet-id-theft-statistics.html
- http://www.consumerfraudreporting.org/pharming.php
- http://www.spamlaws.com/internet-identity-theft
- http://www.identitytheftfixes.com/spyware_can_lead_to_identity_theft.html
- http://www.zdnetasia.com/identity-theft-almost-effortless-in-social-networks-62062905.htm
- http://www.privacyrights.org/fs/fs23-shopping.htm#4
- http://www.staysmartonline.gov.au/factsheets/factsheet_9
- http://www.sec.gov/investor/pubs/onlinebrokerage.htm
- http://ebay.about.com/od/ebaylifestyle/a/el_paypalstudy_2.htm
- http://technofriends.in/2010/11/15/2-firefox-add-on-to-help-you-stay-safe-from-firesheep-security/

INCIDENT REPORTING CHANNELS

Our contact:

Cyber999

Reliable • Effective • Timely

Email	cyber999@cybersecurity.my
Cyber999 Hotline	1 300 88 2999
Fax	603 - 89453442 (monitored during business hours)
SMS	CYBER999 Report <Email> <Complaint> to 15888
H/P	019-266 5850 (24x7 call incident reporting)
Website	http://www.mycert.org.my/

CyberSAFE

Cyber Security Awareness For Everyone

CyberSecurity MALAYSIA

An agency under MOSTI

People First, Performance Now

MOSTI

Ministry of Science, Technology and Innovation

Best Brand Internet Security 2008 & 2009

ISMS SIRIM

CERTIFIED TO ISO/IEC 27001:2005 CERT NO. : AR4656

STANDARDS MALAYSIA

MS ISO/IEC 17025 TESTING SAMM NO. 456

MSC MALAYSIA Status Company

CyberSecurity Malaysia, Level 8, Block A, Mines Waterfront Business Park, No 3 Jalan Tasik, The Mines Resort City, 43300 Seri Kembangan, Selangor Darul Ehsan, Malaysia
www.cybersecurity.my