MENEMBUS BATAS SISTEM DENGAN

EKSPLOITASI PSIKOLOGI USER

Muhammad Ikbal[1)] , Ardhian Agung Yulianto[2)]

[1]Teknik Elektro Universitas Andalas [2]Lembaga Pengembangan TIK (LPTIK) Universitas Andalas

rangsangka@gmail.com[1)] ardhian.ay@ft.unand.ac.id[2)]

ABSTRAK

Tingkat kejahatan dunia maya tumbuh berbanding lurus dengan perkembangan di bidang informasi. Dalam kehidupan sehari-hari yang menuntut user untuk melakukan pekerjaan tepat waktu serta pemanfaatan infrastruktur informasi sesungguhnya telah menjadi ancaman pada suatu hari kemudian. Keamanan pada suatu sistem tidak akan menjamin sepenuhnya user berada pada posisi yang aman, terdapat celah keamanan yang sangat besar yang tanpa disadari bahwa celah keamanan yang bisa di eksploitasi terdapat pada user itu sendiri. Dalam pengamanan data, salah satu teknik yang sangat popular adalah social engineering. Social engineering adalah suatu teknik yang digunakan untuk meyakinkan user agar mendapatkan informasi penting darinya, secara garis besar teknik ini dapat diartikan sebagai salah satu teknik menipu. Dalam pelaksanaannya sendiri, social engineering tidak terlepas dari tindakan pencurian identitas, yaitu penipuan identitas dengan melakukan klaim dirinya sebagai user dengan tujuan mendapatkan keuntungan dari user yang telah dipalsukan tersebut. Untuk dapat melakukan teknik ini dengan baik, seorang penyerang melakukan phising terhadap user/korban, phising atau memancing adalah suatu teknik untuk melakukan suatu penjebakan. Phising memanfaatkan media email, website palsu, spyware dan media lainnya, jika kita perhatikan saat ini salah satu kejahatan penipuan yang sering terjadi adalah dengan memanfaatkan media sms (sort message system). Beberapa hal yang menyebabkan phising ini terus terjadi diantaranya: 1). Ketidaktahuan atau kurang pengetahuan user, 2). Tampilan palsu yang menyesatkan, 3). Kurangnya perhatian pada indikator keamanan.Pada sisi lain, hal yang perlu dipahami secara umum menyangkut system keamanan teknologi informasi adalah tiga aspek penting yang dikenal dengan segitiga CIA, yaitu confidentiality (kerahasiaan), integrity (keutuhan), dan availability (ketersediaan). Confidentiality adalah aspek keamanan yang menyangkut hak akses terhadapat user, integrity adalah haru percaya bahwa informasi yang utuh tidak dimodifikasi selama terjadi proses transaksi informasi dan availability adalah ketersediaan informasi untuk dapat diakses user dalam jangka waktu tertentu. Dari sini nantinya dapat dijadikan acuan untuk melakukan penelitian lebih lanjut mengenai eksploitasi psikologi user.

Kata kunci : social engineerring,kejahatan maya, psikologi, phising

ABSTRACT

The level of cybercrime grows proportional to the developments in the field of information. In daily that requires the user to do the job on time and utilization of infrastructural information has actually become a threat someday. A security on a system will not fully guarantee for user is in a safe position, there is a huge security of hole without realizing that the security of hole can be exploited within the users themselves. In securing a data, one technique that is very popular is social engineering. Social engineering is a technique used to convince the user to obtain a important information from it, an outline of this technique can be interpreted as one of the deceptive techniques. In practice itself, social engineering is inseparable from thief an identity, it is the claim itself as the user in order to benefit from the user that has been forged. To be able to perform this technique properly, an attacker perform phishing for user / victims, phishing or fishing is a technique to perform an entrapment. Phishing email using the media, fake websites, spyware and other media, if we look at this one of a fraud crime is often the case with the media using a SMS (sort message system). Some of the things that led to this phishing attack continue to take place between them: 1). Ignorance or lack of knowledge of the user, 2). False appearance of misleading, 3). Lack of attention to the security indicators, in other hand, things that need to be understood in general concerning information technology security system are three important aspects, known as the CIA triangle, they are confidentiality, integrity and availability. Confidentiality is the security aspects related to user access rights, integrity is to believe that the full information is not modified during the transaction process is the availability of

information and the availability of information to be available to users in a given time period. From here, it will be used as a reference for further research on the exploitation of user psychology.

Key : social engineering, cyber crime, phising, psychology, phising

1. Pendahuluan

1.1. Latar Belakang Masalah

Dalam keamanan suatu sistem, aspek keamanan terhadap piranti keras dan piranti lunak untuk menangkal berbagai serangan seperti *fire wall*, anti virus, dan lain sebagainya. Namun, jika manusia yang menggunakan maupun yang mengoperasikan lalai maka seluruh peralatan canggih yang digunakan untuk menangkal berbagai serangan akan menjadi tidak berati.

Dalam perkembangannya, muncullah suatu metode untuk mengeksploitasi suatu sistem dari sisi user. Metode ini dikenal dengan *social engineering*. Untuk mendapatkan informasi penting dan kruasial yang disimpan oleh manusia.

Dalam segitiga *Confidentiality, Integrity, and Availability* (CIA) kita mengenal tiga aspek penting yang saling berkaitan mengenai keamanan dalam suatu sistem, yaitu: kerahasiaan, keutuhan, dan kesediaan. Kerahasiaan merupakan aspek yang menyangkut pemberian hak akses kepada *user*. Bagi *user* yang belum atau tidak mempunyai hak akses, terlebih dahulu harus mendapatkan hak akses tersebut. Keutuhan merupakan aspek yang menyangkut kepercayaan bahwa informasi yang diakses adalah benar informasi yang "utuh" sesuai dengan yang asli. Utuh, dapat diartikan informasi tersebut tidak berubah dan dimodifikasi dalam proses. Terakhir, ketersediaan adalah aspek yang menyangkut bahwa informasi harus selalu tersedia setiap saat untuk diakses oleh penggunanya.

Gambar 1. Segitiga CIA

1.2. Tujuan dan Manfaat Penelitian

Tujuan dan manfaat penelitian ini adalah sebagai berikut.

1) Menumbuhkan kesadaran user dalam melakukan transaksi elektronik.
2) Menumbuhkan kehati-hatian user dalam menggunakan dan mengakses media online eletronik.

1.3. Perumusan Masalah

Adapun perumusan masalah dalam penelitian ini adalah sebagai berikut.

1) Bagaimana berperilaku yang benar dalam menggunakan media online elektronik

2. Landasan Teori

2.1. Social Enginering

Apabila ditinjau dari segi psikologi, setidaknya ada enam sifat dasar manusia yang dapat menjadi ancaman dan dapat mendorong terjadinya *social engineering*, yaitu.

1) *Reciprocation* (Timbal Balik).
   Dalam kehidupan, khususnya kehidupan bermasyarakat, kita sebagai manusia pasti melakukan interaksi satu sama lainnya karena manusia adalah makhluk sosial yang tidak bisa hidup tanpa bantuan orang lain.
2) *Consistency* (Konsistensi).
   Contohnya, ketika kita mengajukan sebuah pertanyaan dan kemudian menunggu jawabannya, kita tentu akan merasakan kalau diri kita sedang ditunggu. Sifat ini juga dimanfaatkan oleh pelaku *social engineering* untuk mengekploitasi targetnya.
3) *Social Validation* (Validasi Sosial).

Sifat ini lebih identik dengan sifat meniru perbuatan seseorang. Apa yang kita lakukan jika melihat seseorang dijalan dan tiba-tiba melihat satu arah dengan serius ? Yang kita lakukan tentu saja akan melihat ke arah yang sama. Benar bukan ?

4) *Liking* (Kesukaan)
   Kita tentunya akan mengatakan jawaban 'ia' terhadapa apa yang kita sukai dan mengatakan 'tidak' terhadap apa yang tidak kita suka. Atas dasar inilah para peretas sering kali mengekploitasi *user*.
5) *Authority* (Otoritas).
   Apakah kita akan langsung percaya pada seorang ahli dalam mengemukakan penemuan barunya, maka dapat di pastikan kita mempercayainya. Ahli tersebut bagi kita adalah orang yang mempunyai otoritas dalam temuannya. Sifat inilah yang tidak dapat kita pungkiri, karena biasanya kepada siapa lagi kita akan percaya kalau bukan kepada ahlinya.
6) *Scarcity* (kelangkaan).
   Jika manusia dalam keadaan takut,cemas, seperti takut data pentingnya di curi oleh peretas. Setelah mengalami rasa takut/cemas, biasanya manusia akan lebih mudah untuk di eksploitasi.

Social engineering bisa dideskripsikan sebagai suatu cara yang dapat dilakukan untuk meyakinkan orang agar mendapatkan informasi penting darinya. Teknik ini secara kasar mungkin bisa diartikan sebagai teknik menipu karena *social engineering* sangat dekat dengan teknik penipuan. Sebagai contoh, seorang karyawan bisa memberik*an password* kepada seorang *hacker,* dimana sebelumnya *hacker* tersebut melakukan eksploitasi dan pendekatan psikologi karyawan tersebut.[1]

Kategori *social enginerring*[1]

1) Human-based
   Dalam teknik ini, pelaku *social engginerring* berhubungan langsung dengan korbanya. Adapun kategori dari jenis serangan ini adalah sebagai berikut.
   a. *Human based social engineering*.
   b. Berpura-pura menjadi *user*.
   c. Berpura-pura menjadi orang penting.
   d. Berpura-pura menjadi *technical support.*
   e. Menjadi orang yang diberikan kuasa.
   f. Pengintaian.
   g. *Shoulder surfing*.
   h. *Dhumpster diving*.
   i. *Tailgating*.
   j. *Piggy Backing*.
2) Computer-based social engineering
   Social engineering juga dapat dilakukan melalu media computer tanpa berinteraksi langsung dengan korbannya. *Computer-based social engineering* dibagi menjadi beberapa kategori berikut ini.
   a. Instan chat messenger
   b. Pop-up windows
   c. Surat berantai (*chain letter*) dan *hoaxes*
   d. Email spam
   e. Phising

Media yang digunakan dalam *social engineering*[1]

1) Online
2) Telepon
3) Pendekatan personal
4) Reverse social engineering

2.2. Phising

Phising dapat diartikan sebagai suatu teknik serangan untuk menggiring *user* atau korban ke dalam sebuah jebakan. Tujuan dari *phising* adalah mendapatkan informasi penting dari *user* seperti: *akun online* media, *password online* media, pin rekening e-banking, dan lain sebagainya. *Phising* memanfaatkan media email, website palsu, *spyware*, serta berbagai media lainnya.

Metode *phising* [1]

Metode yang sering digunakan diantaranya :

1) *Email/Spam*.
   Media ini terbilang banyak digunakan bahkan bisa dikatakan sebagai media favorit digunakan untuk mencari korban. Email dipilih karena murah dan mudah untuk digunakan. Pelaku bisa mengirimkan jutaan email setiap harinya tanpa perlu mengeluarkan biaya besar.
2) *Web-based Delivery*.
   Pelaku membuat website yang mirip dengan website-website terkenal suntuk mengelabuhi korbannya.

3) IRC/*Instant Mesaging*.
4) Trojan.

Teknik serangan

1) *Man-In-the-Minddle*.
   Hacker menempatkan dirinya ditengah-tengah antara korban dan *website* asli yang hendak diakses. Jenis serangan ini banyak terjadi ketika *user* mengakses media *online* elektronik di lingkungan jaringan lokal, jaringan internet global, dan *wifi.* Salah satu jenis serangan ini adalah melakukan penyadapan terhadap computer *user*.
2) *URL Obfuscation.*
   Metode ini menyamarkan alamat URL sehingga tampak tidak mencurigakan untuk pengguna. Kita dapat pastikan *user* tidak akan melakukan pemeriksaan terlebih dahulu terhadap alamat URL yang hendak dikunjungi.
3) *String* yang menyesatkan.
   Memanfaatkan *string* yang tampak asli dan menggunakan nama besar beberapa perusahaan IT ternama seperti "Microsoft", pelaku membuat direktori yang menggunakan kata-kata Microsoft seperti http://situs.com/microsoft.com/login.aspx
4) Menggunakan tanda "@".
   Tanda "@" jika digunakan dalam suatu alamat URL dapat menipu *user* karena dapat mengantarkan *user* ke halaman palsu yang telah dipersiapkan oleh *hacker*.
5) Status bar yang panjang.
   Teknik ini hamper mirip dengan teknik nomor tiga. *Hacker* menggunakan alamat URL yang panjang yang pada akhirnya dengan kelengahan *user*, maka *user* dapat dipastikan tidak akan melakukan pemeriksaan terlebih dahulu terhadap URL tersebut.
6) Nama yang mirip.
   Hacker membuat sebuah nama yang mirip, misalkan nama *website* perusahaan besar, *website online banking.* Sebagai contoh pada kasus *klikbca.com*, *hacker* bisa membuat website *kilikbca.com*, *klickkbca.com* dan lain sebagainya.
7) URL yang diacak.
   Dalam teknik ini *hacker* mengganti karakter-karakter yang digunakan dalam format lain yang membingungkan.
8) URL *Redirection*.
   Teknik ini memanfaatkan fasilitas *redirect* dari situs asli. Banyak *website* yang mengimplementasikan fasilitas *redirect* ini untuk membantu penggunanya dan apabila tidak dijaga dengan baik, fasilitas ini dengan mudah bisa menjadi serangan balik untuk *website* tersebut.
9) Pemendek URL.
   Pemendek URL yang terkenal seperti *tinyurl.com* sejatinya digunakan untuk membantu *user* dalam mengakses halaman URL yang panjang menjadi alamat URL yang mudah untuk diingat dan dihafal. Tinyurl.com dalam kasus ini, *user* tidak lagi memperhatikan alamat asli yang digunakan.
10) Gambar yang menyesatkan.
    Hacker atau pelaku *phising* membuat halaman yang menyesatkan seperti gambar *address bar* halaman *login* suatu *e-banking* yang mana dengan menggunakan kode kusus *hacker* menyembunyikan *address bar web browsing* yang asli.
11) *Cross-Site Scripting*.
    Serangan ini dilakukan dengan memasukkan kode ke dalam *website* perantara yang akan dijalankan oleh *website* perantara.
12) *Hidden Attacks.*
    Serangan ini memanfaatkan kode-kode yang tersembunyi sehingga tidak terlihat secara visual.
13) *Client-Side Vulnerabilities*.
    Jenis serangan ini adalah dengan memanfaatkan kelemahan yang ada pada *website* atau *server* untuk memasukkan kode program jahat. Dengan kode program jahat ini, target *hacker* adalah untuk melakukan penipuan kepada *user* yang mengakses *server* tersebut.
14) *Malware-Based Phising*.
    Pelaku *phising* atau *hacker* dalam teknik ini memanfaatkan *malware* untuk menyerang computer pengguna atau korban. *Malware* yang terinstall ke dalam komputer korban, bisa melakukan banyak hal sesuai dengan keinginan pelaku *phising*. Beberapa fungsi yang sering dijalankan :
    a. *Keyloger* adalah mencuri ketikan *keyboard computer* korban untuk mendapatkan *password* atau pun informasi berharga lainnya.
    b. *Screen logger* adalah aksi mencuri tampilan layar biasa digunakan untuk melihat apa yang sedang ditampilkan di depan monitor komputer *user*.
    c. *Web trojan* adalah *malware* yang telah terinstall di dalam komputer korban akan memunculkan *pop-up windows* seolah-olah berasal dari *website* yang sedang dikunjungi.

15) DNS *Poisoning.*
DNS dari *user* dirubah agar *user* tidak menyadari bahwa dirinya telah dibawa ke halaman palsu.
16) DNS-*Based Phising*.
Jenis serangan ini hamper mirip dengan jenis serangan sebelumnya.
17) *Content-Injection Phising.*
Pelaku *phising* atau *hacker* merubah isi *website* yang ditampilkan agar tampak seperti berasaal dari *website* yang sebenarnya.
18) *Search Engine Phising.*

3. Pemaparan Penelitian

3.1. Batasan Masalah

Dalam melakukan penelitian ini untuk mendapatkan hasil yang akurat, maka peneliti membatasi masalah ini dalam ruang lingkup sebagai berikut ini.

1) *User* yang mengakses *social media online*, seperti: *Facebook, twitter*.
2) *User* yang mengakses situs berita *online.*
3) *User* yang *mendownload content*, serta *content* bajakan (*software*, lagu, film dll).
4) *User* yang sekedar *browsing*.

3.2. Sampel Data

Dalam penelitian ini, sampel data yang diambil adalah mahasiswa Universitas Andalas yang melakukan akses internet di ruang ICT .

3.3. Metode Pengujian

Metode pengujian yang dilakukan adalah dengan memberikan kuesioner kepada mahasiswa Universitas Andalas. Jumlah mahasiswa yang dilibatkan dalam pengambilan data adalah sebanyak 30 mahasiswa.

4. Hasil dan Diskusi

Pada bagian ini, penelitian dilakukan dengan memberikan kuesioner. Dengan kuesioner ini, kita dapat melihat beberapa hal dari *user* adalah sebagai berikut.

1) Ketidak tahuan atau kurang pengetahuan *user.*
2) Kelengahan *user* terhadap tampilan palsu yang menyesatkan
3) Kurangnya perhatian *user* pada indikator keamanan.

4.1. Bagian *Social Engineerring*

Dalam penelitian ini, didapatkan hasil bahwa kecendrungan *user* dalam menggunakan *media social* sangat besar, *user* cenderung menggunakan Yahoo! Messenger, Facebook chating, IRC dan beberapa media online lainnya untuk berkomunikasi. Media *social* ini adalah salah satu media yang menjembatani *user* untuk dapat melakukan hubungan timbal balik dalam berkomunikasi namun, *user* tidak begitu mengenal lawan bicara mereka hal itu didapatkan hasil 69.93% koresponden tidak mengenal dan ragu-ragu terhadap lawan bicara mereka di *media social.* Jika demikian, eksploitasi terhadap *user* dapat dilakukan dengan berbagai metode pendekatan-pendekatan.

Facebook dalam hal ini sebagai media social yang berbasiskan konten web 2.0 yang mana seluruh isi dari web ini ditulis dan diisi sepenuhnya oleh *user.* Jika kita kaji dari segita *Confidentiality, Integrity, and Availability* (CIA), Facebook harus dapat menjaga kerahasiaan data-data *user* misalkan dengan menyediakan fasilitas pengaturan *privacy* sehingga user dapat mengkontrol informasi apa yang dapat dibagikan kepada publik, kedua mengenai keutuhan, keutuhan data juga sangat diperlukan agar data tersebut dapat sampai dengan benar, dan terakhir adalah kesediaan, artinya website *media social* Facebook dapat diakses oleh seluruh pengguna, jika terjadi gangguan pada salah satu server, maka dapat digantikan oleh server yang lain.

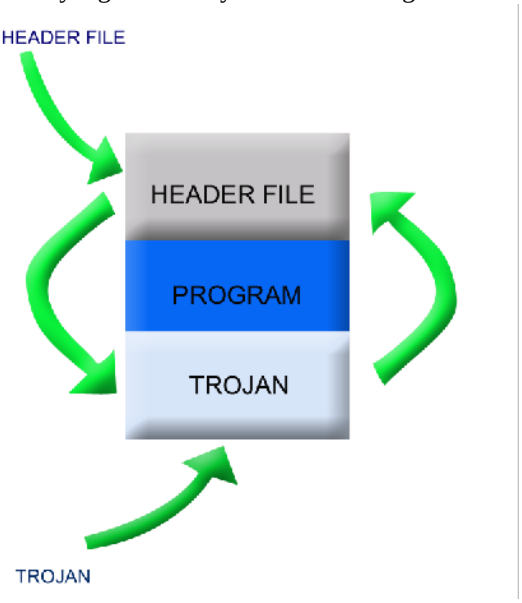
Scarcity (kelangkaan) yang merupakan salah satu sifat dasar manusia dalam kasus ini adalah rasa cemas dan ketakutan akan data yang hilang. Setelah mengalami rasa takut ini, maka dengan teknik pelaku *social enginerring* akan membawa korban kedalam alam bawah sadar dengan memberikan solusi yang sebenarnya adalah jebakan untuk *user* itu sendiri. Sebanyak 23,31% dari 30 korespondensi yang kami pilih menyatakan akan mengikuti saran dari suatu pesan yang menyatakan akun Facebook dalam keadaan bermasalah dan perlu ditindak lanjuti.

Gambar 2. Jebakan untuk menggamankan akun Facebook

4.2. Bagian Phising

Dari hasil survei yang telah dilakukan, didapatkan hasil bahwa user sangat sering mengunduh berbagai macam konten seperti lagu, gambar, video, *software*, dan lain sebagainya. Dalam suatu teknik *hacking* dikenal suatu teknik yang dapat menyisipkan suatu file kedalam suatu file teknik ini dikenal dengan nama *binders*. Dalam penelitian ini peneliti mengambil contoh dari kebiasan mengunduh *software* bajakan, dimana cara kerjanya adalah program akan menyalin Trojan dan diletakkan dibawah suatu program file kemudian merubah *header* dari program untuk memerintahkan komputer mengeksekusi program Trojan terlebih dahulu. Pada akhir program Trojan, akan dibuat lagi sebuah lompatan balik yang akan mengeksekusi program. Dengan begitu, Trojan akan dijakankan secara diam-diam untuk selanjutnya program akan dijalankan secara biasa.[2]

Hacker melalui teknik *binders* dapat memasukkan *spyware, malware, Trojan, key loger* dan lain sebagainya jika suatu *key logger* masuk kedalam komputer korban dapat dipastikan seluruh ketikkan papan keyboard korban akan dapat dibaca oleh *hacker*. Begitu juga dengan *spyware, malware, Trojan, hacker* dapat mengendalikan dan mencuri data-data korban. Dengan kecanggihan program yang telah dirancang *hacker,* misalkan program untuk mematikan antivirus, *fire wall*, maka sistem yang sebelumnya telah dirancang sedemikian rupa akan menjadi sia-sia.



Gambar 3. Proses kerja bindera pembungkus trojan

5. Kesimpulan

Secara umum, dari penelitian ini dapat peneliti simpulkan sebagai berikut ini:

- Dari penelitian ini kami berkesimpulan bahwa user cukup berhati-hati, namun tidak mengurangi celah keamanan.
- Pemakai komputer menyukai penggunaan aplikasi internet yang merepresentasikan diri dan menunjukkan sikap personalnya.

- Keamanan suatu sistem sangat tergantung juga dengan sikap dan perilaku seorang *user* untuk menggunakan dan memanfaatkan fasilitas informatika.

Secara khusus, selanjutnya dari penelitian ini peneliti menyimpulkan beberapa perilaku yang seharusnya dimiliki oleh seorang *user* adalah sebagai berikut ini :

1) Mengatur *prifacy* akun website *social network*
   Dengan melakukan pengaturan *prifacy* terhadap akun *social media* seorang *user* dapat mengendalikan akun. Sebagai contoh, mengatur hanya teman yang telah bergabung dalam lingkaran pertemanan yang dapat melihat profil, foto, dan lain sebagainya. Ini dapat mencegah terjadinya pengintaian dan bahkan pencurian informasi.
2) Dalam lingkaran pertemanan, *user* memiliki kesadaran untuk mengenali lawan bicara
   Pada dunia maya, penipuan dengan mudah terjadi, seseorang dapat berbohong, ataupun memalsukan identitas mereka. Dari hasil penelitian ini didapatkan peserta kuesioner mengakui tidak begitu mengenal lawan bicara. Mengenali lawan bicara harus dilakukan dengan teliti,
3) Jangan cepat terpengaruh oleh iklan, maupun iklan pop-up
   Waspada dan selalu berhati-hati dalam melakukan transaksi elektronik seperti tidak cepat terpengaruh oleh iklan penawaran maupun iklan yang tiba-tiba saja muncul atau yang lebih sering disebut pop-up. Bahaya yang dapat muncul ketika *user* mengklik iklan tersebut adalah *user* diarahkan kepada suatu website jebakan (*phising*), ataupun diarahkan kepada suatu website/server yang telah disiapkan didalamnya berupa *malware.*
4) Tidak sembarangan melakukan klik
   Dalam hal ini diharapkan kepada *user* untuk tidak sembarangan mengklik attachment email atau mengklik link yang tidak diketahui sumbernya. Pertumbuhan *email spam* akhir-akhir ini sangat meresahkan terlebih lagi jika *user* tidak mengetahui apa itu *email spam,* dampak apa yang akan terjadi. Dengan menggunakan *social engineering,* seorang *hacker* dapat melakukan penipuan, menyebarkan *worm.*
5) Tidak sembarangan mengunduh
   Ketika hendak mengunduh, *user* terlebih dahulu mengenali website tersebut, apakah website tersebut benar-benar adalah website terpercaya, membaca semua peringatan keamanan, persetujuan lisensi, dan *prifacy* terkait konten yang akan di unduh. Kebiasaan yang salah selama ini adalah user sering mengunduh aplikasi, maupun konten bajakan. Selain melanggar hak cipta, pada software bajakan tersebut tidak menutup kemungkinan telah terlebih dahulu dimasukkan program jahat.
6) Melakukan *update* berkala dan melakukan cek terhadap *path* piranti lunak yang digunakan
   Adapaun *update* serta *path* ini disediakan oleh vendor penyedia untuk melindungi komputer user dari virus dan celah keamanan tertentu.

DAFTAR PUSTAKA

[1] Sto. 2011. *Certified Ethical Hacker 400% illegal.* Jasakom Publishing: Jakarta.
[2] Sto. 2010. *Certified Ethical Hacker 300% illegal.* Jasakom Publishing: Jakarta.
[3] Sto. 2004. *Seni Teknik Hacking 1 (Uncensored).* Jasakom Publishing: Jakarta.
[4] Sto. 2004. *Seni Teknik Hacking 2 (Uncensored).* Jasakom Publishing: Jakarta.

[5] http://ictwatch.com/internetsehat/2012/07/30/hampir-50-user-malas-update-software/

akses terakhir pada hari senin, 10 September 2012 jam 21:20 wib

[6] http://ictwatch.com/internetsehat/2011/11/02/8-perilaku-wajib-berkomputer-sehat/

akses terakhir pada hari senin, 10 September 2012 jam 21:20 wib