STUDI ISU KEAMANAN JARINGAN PADA FACEBOOK

Rifqy Hakimi[1]
[1]Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung,
email: rifqyhakimi@gmail.com

ABSTRAK

Facebook merupakan salah satu media jejaring sosial yang terlaris di Indonesia bahkan di dunia. Jejaring sosial ini digunakan untuk berinteraksi dengan relasi, teman, berbagi foto, dan bahkan untuk mengembangkan bisnis. Pada paper penelitian ini akan dibahas isu keamanan yang bisa mengancam pada Facebook. Serangan yang bisa mengancam keamanan data pribadi pada Facebook antara lain *phising*, *clickjacking*, dan *link scam*. Dalam paper ini akan dianalisis cara kerja serangan dan penanganan serta pencegahan yang dapat dilakukan terhadap serangan ini.

Kata Kunci : Facebook, *phising, clickjacking, link scam*

Pendahuluan

Facebook merupakan salah satu media jejaring sosial yang terlaris di Indonesia bahkan di dunia. Di Indonesia, Facebook sudah menjadi gaya hidup yang tidak terpisahkan. Jejaring sosial ini digunakan untuk berinteraksi dengan relasi, teman, berbagi foto, dan bahkan untuk mengembangkan bisnis. Facebook merupakan salah satu fenomena yang telah berkembang pesat dalam sejarah internet belakangan ini.[1]

Oleh karena itu, diperlukan pemahaman terhadap isu keamanan data dan ancaman yang terdapat pada Facebook. Pemahaman ini diperlukan untuk kewaspadaan dan pencegahan terhadap serangan ini.[2]

Pada paper penelitian ini akan dibahas isu keamanan yang bisa mengancam pada Facebook. Serangan yang bisa mengancam keamanan data pribadi pada Facebook antara lain *phising, clickjacking,* dan *link scam*. Dalam paper ini akan dianalisis cara kerja serangan dan penanganan serta pencegahan yang dapat dilakukan terhadap serangan ini.

Isu Keamanan pada Facebook

Terdapat banyak jenis serangan yang bisa mengancam keamanan jaringan pada aplikasi jejaring sosial seperti Facebook. Akan tetapi, dalam paper ini akan dibahas tiga serangan antara lain : *phising, clickjacking,* dan *link scam*.

Phising Attack

Phising merupakan suatu teknik serangan dengan menggunakan kamuflase yang membujuk korban agar memberikan informasi pribadi yang sangat berharga seperti nomor kartu kredit, nomor rekening bank, dan lain-lain

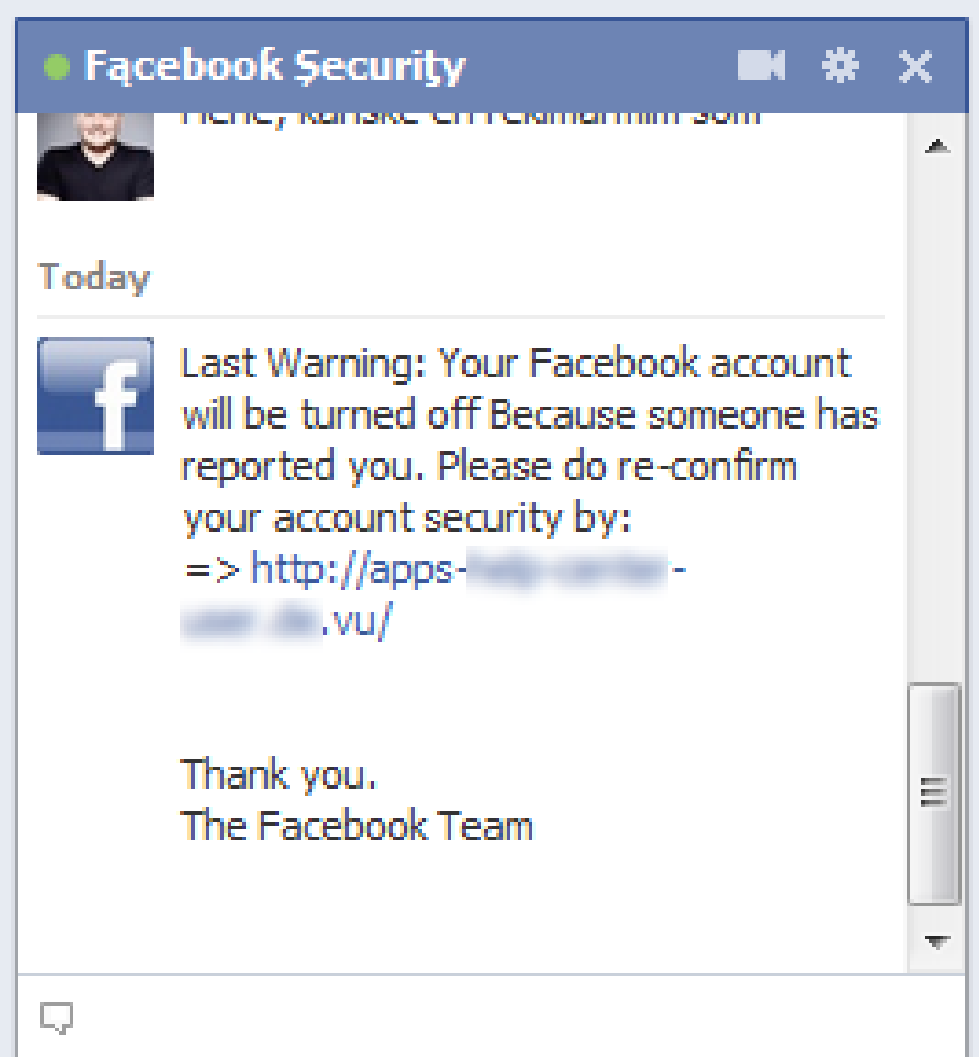
Phising umumnya dilakukan melalui media antara lain :

a) Email *phising*
b) Website *phising*

Serangan *phising* terbaru pada Facebook dilaporkan terjadi pada awal tahun 2012 seperti yang dilaporkan oleh David Jacoby, seorang ilmuwan di Lab Kaspersky, pada 13 Januari 2012.[3] Serangan yang dilancarkan tidak hanya mencuri Facebook *credential,* tetapi juga informasi-informasi penting seperti kartu kredit, dan informasi pertanyaan sekuriti yang biasanya digunakan untuk validasi pada saat kelupaan *password* untuk *log in*.

Serangan *phising* ini tidak hanya mengelabui si korban agar mengunjungi suatu website yang penuh jebakan, namun si penyerang akan menggunakan informasi yang telah berhasil dicuri untuk *log in* ke akun si korban dan mengganti *profile picture* menjadi logo Facebook serta mengganti nama account menjadi "Facebook Security".

Setelah berhasil berkompromi dengan suatu akun korban, maka si penyerang juga akan melakukan *broadcast* suatu pesan ke semua kontak yang dimiliki oleh akun tersebut seperti terlihat pada gambar di bawah ini :



Gambar 1. Pesan yang di*broadcast* ke semua kontak pada akun yang telah dibobol [3]

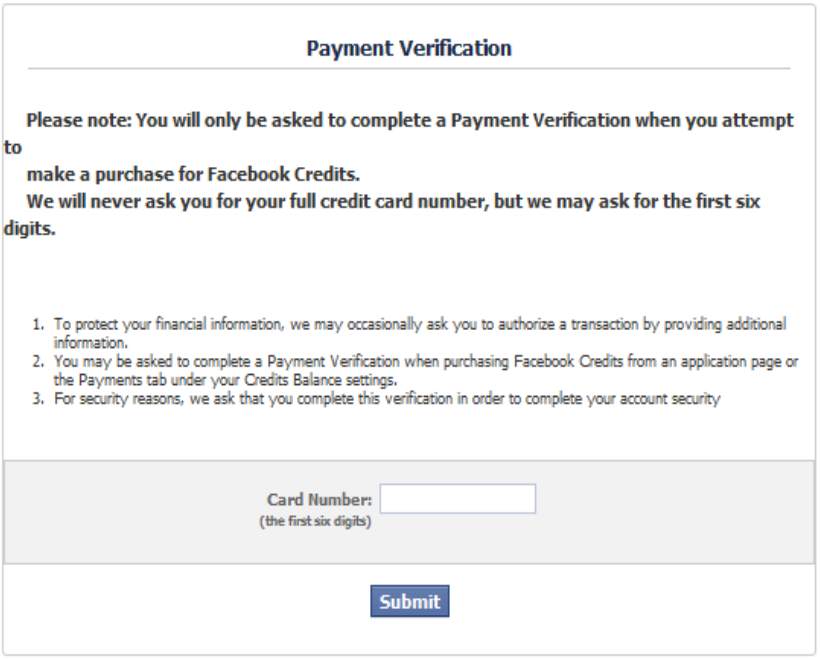
Tulisan dari pesan tersebut berbunyi suatu peringatan bagi teman korban mengenai keaslian akun si teman korban tersebut. Karena peringatan tersebut, si teman korban harus melakukan konfirmasi tentang keaslian akun miliknya sendiri, jika tidak ingin akun miliknya dinonaktifkan oleh si pengirim peringatan tersebut yang mengaku dari "Facebook Team".

Celah inilah yang dimanfaatkan untuk mengelabui si teman korban untuk menjadi korban berikutnya dengan mengarahkan si teman korban untuk mengkonfirmasi keaslian *akun*Facebook miliknya dengan mengunjungi halaman web yang telah dikamuflase. Ketika si teman korban mengklik link untuk konfirmasi yang tertera pada pesan tersebut, maka si teman korban akan diarahkan ke website yang dikamu-flasekan sangat mirip dengan web Facebook, dan diminta untuk mengisi informasi pribadi seperti nama, alamat email, password, dan sebagainya. Berikut tampilan halaman web tiruan Facebook tersebut.

Gambar 2. Tampilan website tiruan Facebook [3]

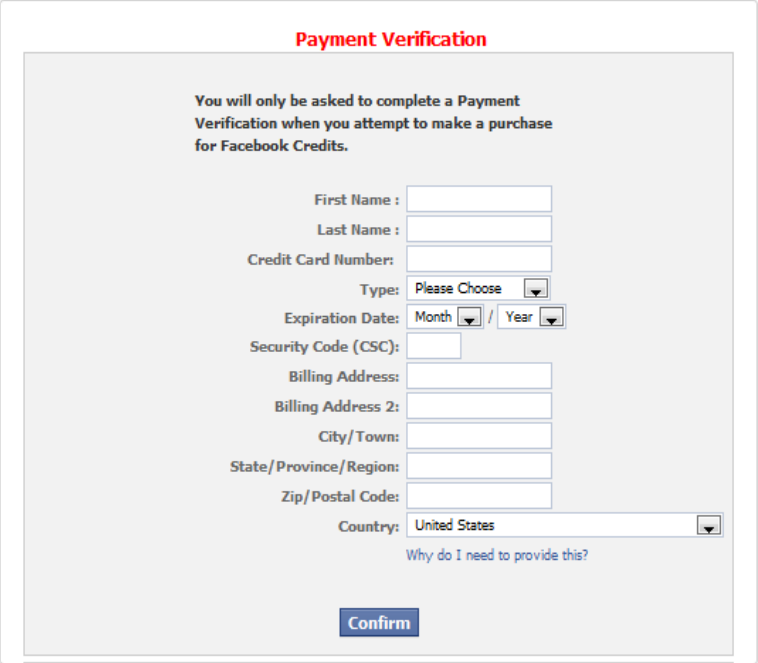
Ketika si teman korban mengisi formulir identitas di atas, lalu di*submit* ke si penyerang, maka si penyerang akan dapat log ini ke akun si teman korban yang telah menjadi korban baru dalam serangan ini.

Setelah si korban baru melakukan konfirmasi dengan mengisi identitas pribadi tersebut, maka halaman web baru akan muncul. Halaman web ini menyatakan bahwa si korban perlu untuk melakukan konfirmasi identitas dengan mengidentifikasi sistem pembayaran seperti kartu kredit. Si korban pun diminta untuk memasukkan nomor kartu kreditnya seperti yang terlihat pada gambar berikut ini.



Gambar 3.Tampilan website tiruan Facebook yang meminta informasi kartu kredit [3]

Kemudian, halaman beriktunya akan mencul dan menampilkan konfirmasi kartu kredit korban yaitu validasi kode Card Security Code (CSC) maupun Card Verifification Value (CVV).



Gambar 4. Tampilan website tiruan Facebook yang meminta konfirmasi kode keamanan kartu kredit [3]

Serangan phising seperti ini patut diwaspadai oleh pengguna Facebook. Oleh karena itu, diharapkan jangan sekali-kali memberikan informasi pribadi seperti email, password, nomor kartu kredit, dan sebagainya pada jejaring sosial.

Clickjacking Attack

Clickjacking attack merupakan jenis serangan yang banyak dilancarkan di Facebook. *Clickjacking* menggunakan aplikasi berbasis web. Sebagian besar dari user tidak menyadari diserang oleh clickjacking ini. Serangan ini cukup rumit karena membutuhkan sedikit skill pemrograman dari si penyerang.

Clickjacking merupakan singkatan dari "Click Hijacking". Dalam serangan ini, penyerang akan membajak tombol klik user. Serangan ini akan mengelabui korbannya untuk melakukan klik pada suatu link yang berbeda dari persepsi user. Serangan ini menggunakan iFrame dan CSS untuk mengelabui korbannya.

Gejala serangan ini dapat dijelaskan dengan lebih mudah. Misalkan, terdapat suatu halaman web X yang sengaja dibuat oleh si penyerang. Pada halaman web ini, si penyerang telah memasukkan iFrame yang diambil dari halaman web Y. Dan frame tersebut didesain sedemikian hingga hanya sebuah tombol dari halaman web Y yang terlihat di halaman web X. Tombol ini pun didesain sedemikian hingga si korban pun yakin bahwa ini merupakan web asli dengan tombol tambahan dari web page Y. Misalkan, web Y itu adalah facebook. Dan web X adalah web jebakan hasil kreasi si penyerang. Web X ini akan menawarkan layanan yang berbeda, dan mengharuskan user untuk klik tombol di web X tersebut. Serangan ini baru bisa berhasil jika user telah login terlebih dahulu.

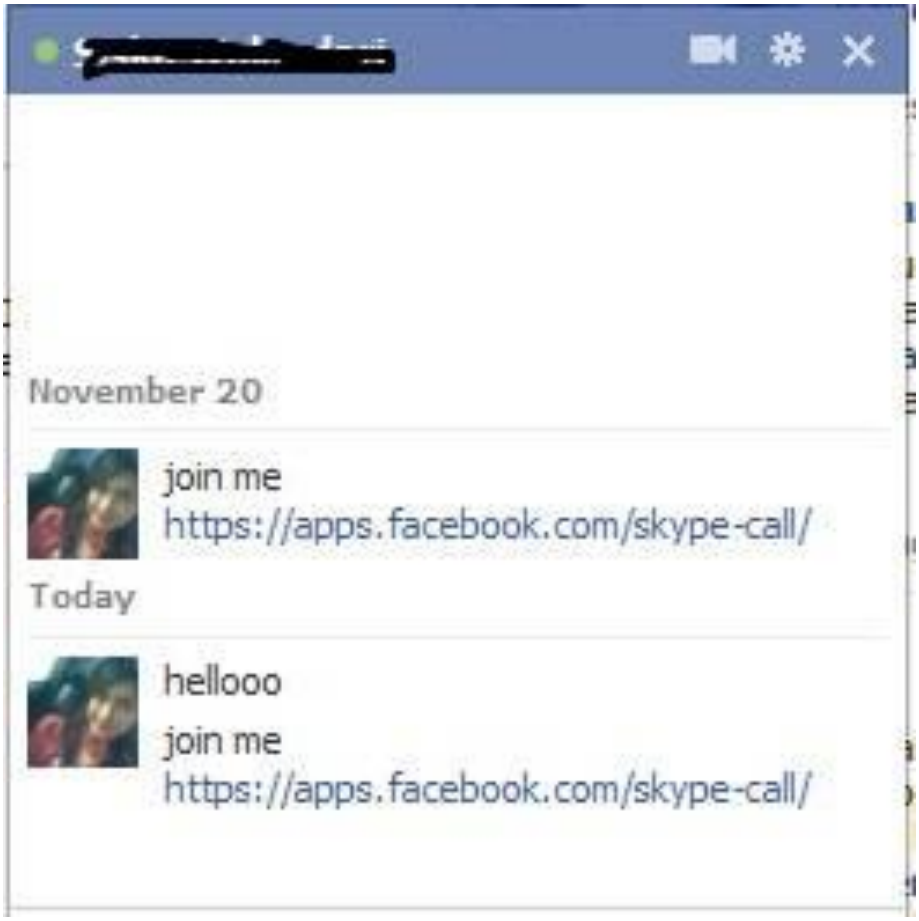
Beberapa bulan yang lalu, dilaporkan terdapat serangan *clickjacking* dengan modus menggunakan halaman web yang berisi video lagu dan terdapat tombol untuk memutar video tersebut [4]. Akan tetapi, terdapat tombol tersembunyi dari situs jual beli Amazon yang dikamuflasekan dibalik tombol pemutar video tersebut. Jika korban melakukan klik pada tombol untuk memutar lagu, maka sebenarnya si korban telah membeli produk di Amazon.

Beberapa tipe serangan yang *clickjacking* ada juga yang memiliki modus yang berbeda. Ketika user melakukan klik pada link dan kemudian akan dibawa ke sebuah halaman web dengan tombol "like" yang tersembunyi. Serangan ini disebut likejacking. Karena tombol like nya disembunyikan dan memungkinkan ditaruh di manapun, dan jika dilakukan klik di manapun pada halaman tersebut, akan menghasilkan feed berita atau posting yang akan di share ke teman-teman pada Facebook secara otomatis. Jika teman si korban melihat hal ini, dan melakukan klik pada link tersebut, maka akan menyebarkan spam tanpa disadari.

Link Scam

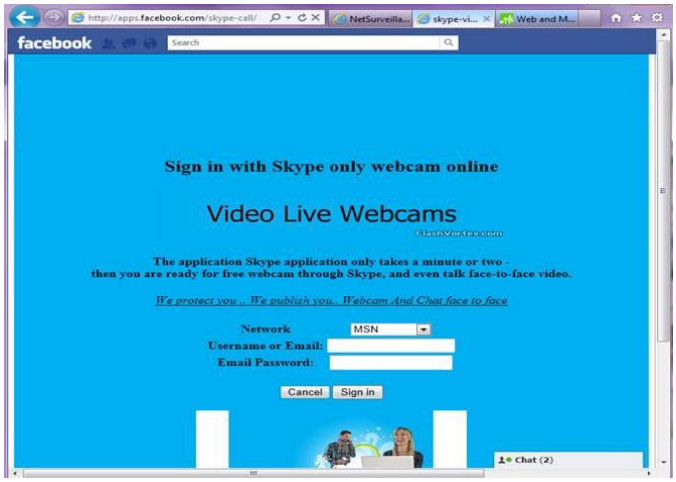
Serangan *clickjacking* umunya juga menggunakan modus link yang disebut scam ini. Akan tetapi, di sini dibahas link scam dengan modus yang berbeda. Link scam ini pada prinsipnya adalah link palsu mirip seperti phising.

Berikut ini merupakan salah satu modus link scam yang mengatasnamakan berasal dari aplikasi baru yaitu Skype Call. Link scam ini dikirim melalui fitur chatting pada Facebook.



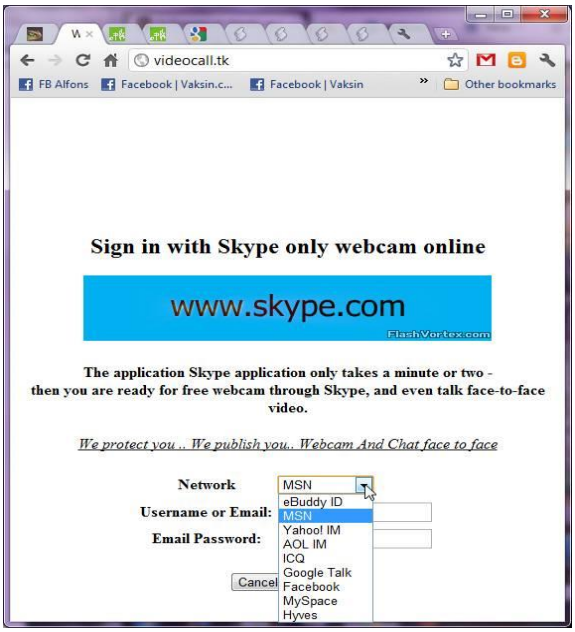
Gambar 5. Pesan Facebook mengenai adanya aplikasi Skyke-Call melalui fitur chatting [8]

Jika link di atas diklik, maka user akan dibawa ke website aplikasi Skype-call yaitu http://apps.facebook.com/skype-call. Berikut ini adalah tampilannya :



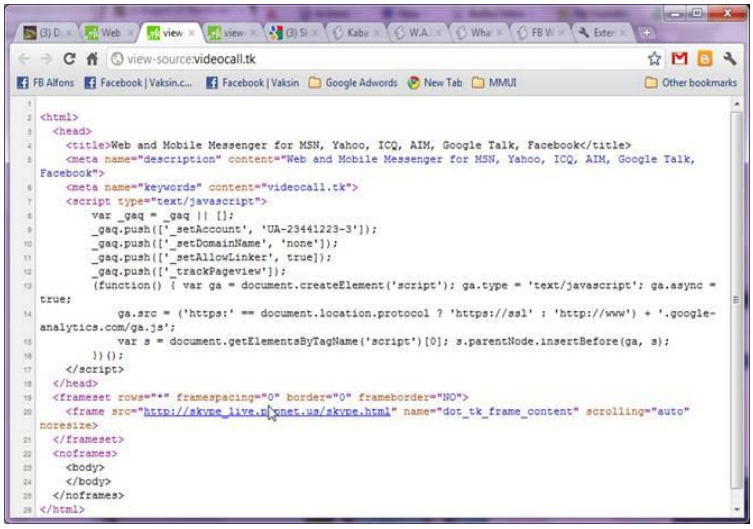
Gambar 6. Tampilan website aplikasi palsu Facebook yaitu Skype-Call [8]

Prosedur yang dilakukan dalam instalasi aplikasi pada Facebook yaitu pertama-tama adalah tampilan konfirmasi permintaan persetujuan pemilik akun untuk menggunakan aplikasi tersebut. Dalam hal ini, konfirmasi persetujuan pemilik akun inilah yang sengaja dilewatkan oleh si penyerang, sehingga korban langsung menuju pada konfirmasi untuk penggunaan Skype Video Live Webcams. Dan korban pun langsung dihadapkan pada pilihan akun yang bisa digunakan untuk login, seperti akun MSN, Yahoo, Facebook, Google Talk, dan lain lain. Berikut ini adalah tampilannya :



Modus ini juga menggunakan teknik *phising*. *Phising* yang dibuat yaitu seolah-olah ini berasal dari Skype asli. Jika menggunakan Facebook dengan mengaktifkan secure browsing atau protokol https, maka frame website ini dianggap seakan-akan merupakan aplikasi Facebook asli. Namun, jika

diteliti lebih dalam source page tersebut, maka akan diketahui bahwa page ini bukanlah berasal dari Skype asli tetapi mengambil frame dari halaman website http://skype_live.p**net.us/skype.html dan kemudian digunakan nama Skype untuk mengelabui si korban. Si penyerang pun telah mempersiapkan page Facebook untuk aplikasi ini disertai dengan logo Skype agar lebih meyakinkan. Berikut ini adalah tampilannya.



Gambar 8. Source page aplikasi Skype Call yang berisi Javascript untuk mencuri password korban [8]

Gambar 9. Page Facebook untuk aplikasi Skype Call dengan logo Skype [8]

Setelah informasi personal korban seperti username dan password beberapa akun, si penyerang akan menggunakan akun Facebook korban untuk mengirimkan pesan melalui fitur Facebook chat ke seluruh kontak teman Facebook korban supaya mengaktifkan aplikasi Skype Webcams ini.

Sekali lagi, untuk mengelabui si korban yang telah diambil informasi username dan passwordnya, maka si penyerang pun akan mengarahkan si

korban untuk menuju ke chatroom pornografi. Hal ini dilakukan si penyerang untuk mengalihkan perhatian si korban agar tidak menyadari bahwa informasi login mereka telah dicuri. Hal ini terlihat pada gambar di bawah ini.

Gambar 10. Tipuan chatroom untuk mengelabui korban [8]

Analisis dan Pencegahan

Terdapat banyak jenis serangan yang bisa mengancam keamanan jaringan pada aplikasi jejaring sosial seperti Facebook. Akan tetapi, dalam paper ini akan dibahas tiga serangan antara lain : *phising, clickjacking,* dan *link scam*. Berikut ini akan dianalisis langkah-langkah penanganan dan pencegahan yang dapat dilakukan jika terjadi serangan tersebut.

Phising Attack

Phising attack cukup merugikan terutama bagi nasabah bank. Ada beberapa hal yang perlu dicermati agar terhindar dari serangan *phising* :

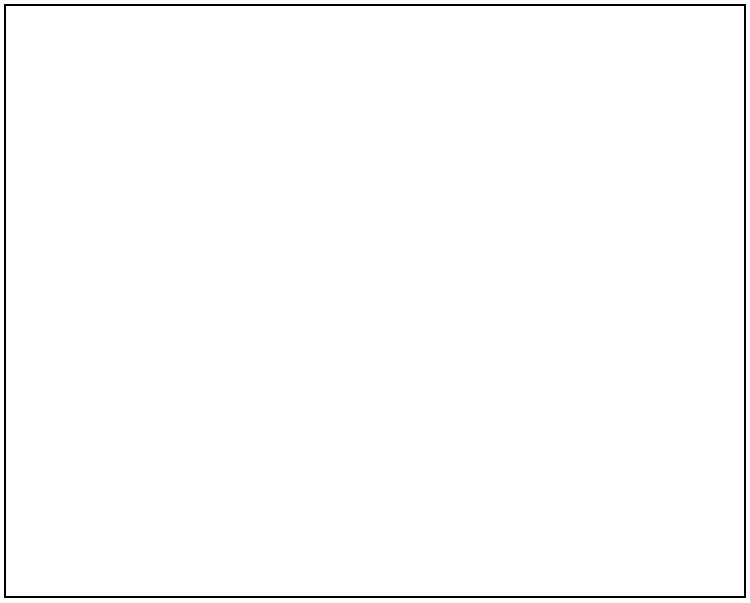
a) Telusuri asal usul email yang diterima.
   Umumnya dalam hal ini, si penyerang menggunakan modus mengirimkan email pancingan ke sejumlah calon korban. Email tersebut biasanya meminta si calon korban untuk mengunjungi website tersebut, kemudian melakukan registrasi ulang dengan memasukkan username dan password e-banking nasabah.
   Jika menerima email yang tipikal seperti ini, diharapkan untuk mengecek terlebih dahulu darimana email tersebut berasal. Pastikan email tersebut menggunakan domain resmi dari bank. Hal ini akan meningkatkan validitas email tersebut benar berasal dari bank tersebut.
b) Informasi registrasi ulang tidak cukup hanya via email.
   Registrasi ulang akun suatu bank tentunya tidak hanya cukup untuk disampaikan lewat email. Hal ini disebabkan informasi penggantian username dan password akun bank merupakan hal yang sangat krusial. Pihak bank akan menghubungi pelanggan yang bersangkutan secara profesional, baik menggunakan email resmi maupun dengan menelpon langsung. Jadi, tidak akan mungkin dengan hanya konfirmasi via email.
c) Menghubungi customer service bank
   Menghubungi pihak bank melalui customer servicenya akan sangat berguna untuk memverifikasi tentang kebenaran prosedur registrasi password ulang.
d) Membedakan website yang asli dengan tiruan.
   Untuk website resmi suatu bank biasanya memiliki tingkat keamanan yang cukup ketat. Website suatu bank menggunakan protokol *Hyper Text Transfer Protocol Secure* (https). Protokol

ini memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan protokol *Hyper Text Transfer Protocol* (http) biasa.

Https merupakan kombinasi dari protokol http dan *Secure Socket Layer* (SSL). Protokol ini mampu menyediakan komunikasi terenkripsi antara web server dan klien. Protokol ini biasanya digunakan pada halaman login, transaksi pembayaran ataupun perbankan, dan sebagainya. Berikut ini adalah contoh tampilan website salah satu bank yang ada di Indonesia, yaitu BNI yang menggunakan protokol https.

Gambar 11.Tampilan website BNI yang menggunakan https [6]

Berikut ini terdapat bukti website suatu bank yang tidak menggunakan protokol https. Website tersebut merupakan website palsu.



Gambar 12.Tampilan website Bank Permata palsu yang tidak menggunakan https [5]

Jika korban telah memasukkan username dan password pada website palsu tersebut, maka data-data ini tentu akan diketahui oleh si penyerang yang menggunakan website ini sebagai modusnya. Dan rekening bank pun terancam bisa dibobol dengan mudah, jika si korban tidak menyadari hal ini.

Hal pertama yang dapat memverifikasi website perbankan tersebut asli adalah dengan melihat protokol https pada websitenya. Kedua,

pada bagian kanan bawah browser seperti contohnya pada Mozilla Firefox, terdapat gambar gembok yang terkunci. Untuk pengguna Internet Explorer terdapat gembok warna kuning di sebelah alamat URL tersebut.

Namun, perlu dicermati bahwa https hanya berfungsi untuk melakukan enkripsi informasi. Contohnya informasi dari kartu kredit yang dimasukkan melalui browser ke web server yang menerima informasi tersebut. Informasi tersebut akan disimpan di dalam database server yang kadang-kadang tidak langsung diteruskan ke operator kartu kredit. Server database ini juga merupakan salah satu sasaran serangan. Oleh karena itu, https bukanlah suatu jaminan mutlak yang melindungi suatu transaksi keuangan.

Clickjacking Attack

Terdapat banyak jenis serangan yang bisa mengancam keamanan jaringan pada aplikasi jejaring sosial seperti Facebook.

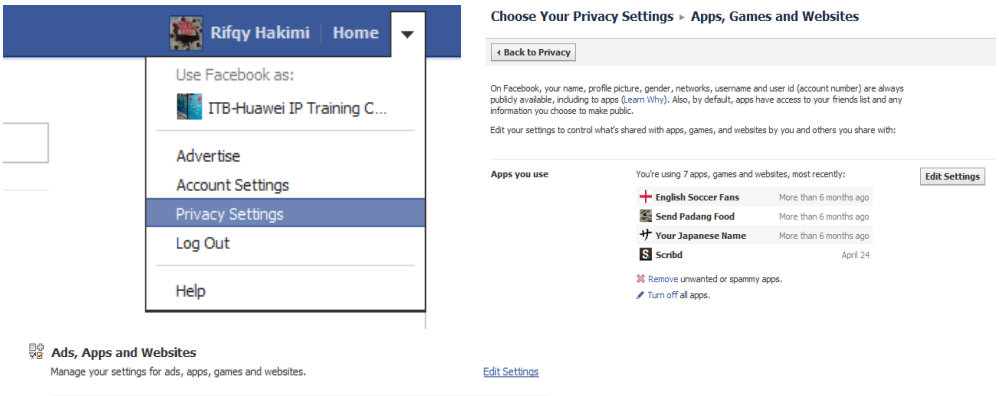
Beberapa tindakan pencegahan dari serangan clikjacking yang muncul pada Facebook antara lain :

a) Waspada terhadap *link scam*
Link scam juga dapat digunakan sebagai modus penyerangan. *Link scam* ini nantinya akan menyerang *wall user* dan memaksa user untuk menyetujui instalasi aplikasi tertentu di Facebook. Aplikasi ini biasanya menyebabkan si user melakukan posting di wall dan page teman dari user tersebut tanpa disengaja.

Langkah-langkah pencegahan dari serangan link scam ini dapat dilakukan dengan:

- Waspada terhadap link pendek yang berasal dari teman yang biasanya tidak pernah share link sebelumnya. Apalagi jika link yang di share banyak sekali. Hal ini patut dicurigai sebagai link scam.
- Jika hendak melakukan instalasi aplikasi, telusuri dan investigasi terlebih dahulu sebelum disetujui untuk dilakukan instalasi. Aplikasi yang terlalu "baik" patut untuk diwaspadai.
- Pengaturan otorisasi aplikasi perlu diperhatikan. Hak posting dari suatu aplikasi perlu untuk dicermati.

Jika link scam telah menyerang suatu akun Facebook, tindakan penanya-ngan yang dapat dilakukan terhadap serangan ini yaitu dengan mem-perhatikan halaman pengaturan privacy. Pada gambar berikut terlihat tampilan "Privacy Setting" pada kanan atas Facebook. Kemudian masuk ke "Ads, Apps, and Websites". Maka terdapat list aplikasi yang digunakan. Jika terdapat aplikasi yang baru saja diaktifkan, tetapi malah menimbulkan masalah, maka aplikasi tersebut dapat dihapus dari sini.



Gambar 13.Tampilan privacy setting pada Facebook

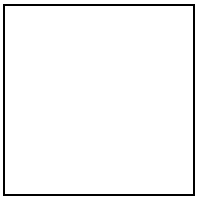
b) Waspada terhadap informasi yang diberikan kepada suatu aplikasi
Aplikasi merupakan salah satu celah yang bisa dimanfaatkan oleh penyerang. Aplikasi umumnya memiliki kemampuan untuk mengetahui alamat email dan informasi personal yang lainnya. Oleh karena itu, waspadalah terhadap pemakaian aplikasi tersebut, dan aplikasi tersebut bisa dihapus setelah digunakan supaya tidak menimbulkan spam.

Link Scam

Penanganan dan pencegahan terhadap serangan *link scam* ini tidak cukup hanya dengan menggunakan antivirus. *Link scam* di sini akan menyerang akun Facebook suatu korban, dan kemudian akan menyebarkannya ke teman-teman korban tersebut, sehingga tidak menutup kemungkinan si teman korban pun akan terjebak dalam lingkaran serangan ini.

Vaksin.com merupakan salah satu kelompok riset yang peduli terhadap ancaman scam ini pada Facebook. Vaksin.com menyarankan beberapa cara pencegahan untuk mengindari dan mengantisipasi serangan *link scam* ini, antara lain dengan cara : [8]

1) Mengaktifkan *secure browsing* seperti https untuk mengakses akun Facebook, maupun akun lainnya.
Protokol https akan mengenkripsi seluruh data yang dikirimkan antara browser dengan server penyedia layanan seperti Facebook sehingga akan sangat menyulitkan si penyerang untuk mencuri informasi personal seperti username dan password login akun.
Pada akun Facebook, secure browsing https dapat diaktifkan dengan cara klik tombol panah ke bawah di sebelah kanan menu "Home", lalu kemudian memilih "Account Settings". Setelah itu dilanjutkan dengan memilih "Security Settings" pada pilihan menu "Security" di sebelah kiri. Kemudian memilih "Edit" pada pilihan menu "Secure Browsing" dan memcentang pilihan "Browse Facebook on a secure connection (https) when possible" lalu setting ini disimpan dengan memilih menu "Save Changes".

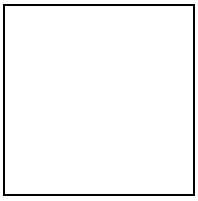


Gambar 14. Mengaktifkan secure broswing https pada Facebook [8]

2) Menggunakan password yang kuat dengan mengkombinasikan karakter huruf besar dan kecil, angka dan huruf, serta tanda baca.
Password yang kuat tidak mudah ditebak dan diganti secara berkala. Jangan menggunakan password yang sama untuk beberapa akun karena hal ini akan melemahkan pertahanan security. Jika password berhasil dicuri maka akun lainnya yang menggunakan password yang sama akan terancam.
Penggunaan pengingat password pun dapat membantu jika ingin memiliki banyak informasi password yang harus diingat. Program pengingat password akun ini akan menyimpan dan mengekripsi semua informasi kredensial seperi username dan password login banyak akun. Dan user pun hanya perlu mengingat satu

password untuk mengakses seluruh password yang disimpan.

3) Menggunakan antivirus yang selalu diupdate.
   Antivirus ini akan melindungi dari serangan Trojan maupun Keylogger yang bisa mengancam password user. Antivirus yang digunakan sebaiknya memiliki kemampuan proteksi web yang bisa mendeteksi dan melindungi dari serangan phising, link scam, dan trojan.



Gambar 15.Contoh antivirus yang memiliki proteksi web [8]

Kesimpulan

Kesimpulan

Adapun kesimpulan yang dapat ditarik dalam studi paper ini antara lain:

1. Serangan yang bisa mengancam isu keamanan Facebook antara lain *phising, clickjacking*, dan *link scam*
2. Pencegahan terhadap serangan *phising* dapat dilakukan dengan cara mewaspadai link dan email yang diterima, menggunakan *secure browsing* https, dan mewaspadai transaksi perbankan agar menggunakan website resmi bank tersebut.
3. Pencegahan terhadap serangan *clickjacking* dapat dilakukan dengan cara mewaspadai link scam, mewas-padai aplikasi yang diinstall dan informasi yang diberikan pada aplikasi tersebut
4. Pencegahan terhadap serangan *link scam* dapat dilakukan dengan cara menggunakan *secure browsing* https, menggunakan password yang kuat, dan menggunakan antivirus yang terupdate dan memiliki proteksi web yang kuat.

Saran

Adapun saran dari penulis untuk pengembangan penelitian berikutnya antara lain:

1) Membuat simulasi serangan *phising*, *clickjacking*, dan *link scam* untuk lebih memahami cara kerja dan mewaspadai jenis dan tipe serangan ini
2) Membahas tipe serangan lain seperti *cursorjacking*, dan *likejacking*

Daftar Pustaka

[1] Brad Dinerman (2011). *Networking Security and Security Risks* http://www.gfi.com/whitepapers/Social Networking and Security Risks.pdf

[2] Harvey Jones, Jos_e Hiram Soltren (2005).*Facebook: Threats to Privacy*

[3] David Jacoby (2012). *Facebook Security Phising Attack In The Wild* http://www.securelist.com/en/blog/208193325/Facebook Security Phishing Attack In The Wild
Waktu akses : 2 Mei 2012, 11.30 WIB

[4] Deepanker Verma (2012). *Clickjacking, Cursorjacking, and Common Facebook Vulnerabilities* http://resources.infosecinstitute.com/clickjacking-facebook/
Waktu akses : 3 Mei 2012, 13.05 WIB

[5] Allien (2010). *Waspada Terhadap Tipuan Phising bagi Nasabah Bank* http://jumper99.blogspot.com/2010/12/waspada-terhadap-tipuan-phising-bagi.html
Waktu akses : 3 Mei 2012, 15.09 WIB

[6] Website Bank BNI https://ibank.bni.co.id/directRetail/ibank?pid=5056505456575448495249485149545150555656
Waktu akses : 4 Mei 2012, 18.00 WIB

[7] Allien (2011). *Waspadalah Pada Clickjacking* http://jumper99.blogspot.com/2011/09/waspadalah-pada-clickjacking.html
Waktu akses : 2 Mei 2012, 11.00 WIB

[8] Aa Tan (2011). *Ancaman Scam Facebook dan Pencegahannya* http://vaksin.com/2011/1211/facebook%20scam/facebook%20scam.htm
Waktu akses : 4 Mei 2012, 09.10 WIB