Computer Security

Josua M Sinambela,
CEH, CHFI, ECSA|LPT, ACE, CCNP, CCNA, Security+
Computer Network & Security Consultant
RootBrain.Com

TEKNOLOGI

Karyawan Google Sebar Exploit di MS Windows

Ormandy menganggap Microsoft tak akan segera meluncurkan program tambalannya.

Indra Darmawan

MINGGU, 13 J

(VIVAnews)

VIVAnews - Se
Google dikecam
sengaja merilis k

BERITA TER

Ribuan Email Pengguna iPad Bocor, FBI Beraksi

Peretas gunakan script penebak nomor ICC-ID iPad. Ribuan email pelanggan AT&T terungkap.

Indra Darmawan

MINGGU, 13 JUNI 2010, 13:11 WIB

VIVAnews - Peristiwa kebocoran sekitar 114 ribu alamat email pengguna iPad, berbuntut panjang. Badan investigasi Amerika Serikat FBI, sampai-sampai merasa perlu turun tangan menyelidiki masalah ini.

Pada Selasa pekan lalu, sebuah cacat di situs web AT&T (operator penyalur perangkat tablet iPad) menyebabkan terungkapnya lebih dari 100 ribu alamat email pembeli iPad di Amerika Serikat.

Beberapa di antara email yang bocor tadi terdapat orang-orang terpandang, seperti Kepala Staf Gedung Putih Rahm Emanuel,

Lewat Status 'Like', Trojan Berbahaya Teror Facebooker

Fajar Widiantoro - detikinet

facebook (ist)

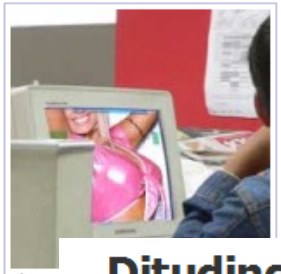
Jakarta - Trojan jenis baru meneror pengguna Facebook. Kali ini modus operandinya melalui sebuah tawaran status 'like'. Jadi jangan sembarangan meng-aprove status 'like' pada situs asing.

Dalam aksinya, trojan tersebut akan memancing pengguna untuk masuk sebuah situs asing dengan pesan secara langsung ke akun Facebooker. Mereka kemjudian akan dipancing untuk meng-klik status 'like'. Berikut ini adalah beberapa pesan yang dicurigai disusupi trojan tersebut.

"LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE," "This man takes a picture of himself EVERYDAY for 8 YEARS!!," "The Prom Dress

Virus Sesatkan Pengguna Akses Situs Porno

Ardhi Suryadhi - detikinet



Jakarta - Setelah dihebohkan dengan video porno mirip artis, dunia internet Indonesia kembali mendapat ancaman virus yang menjerumuskan para korbannya ke situs porno.

Menurut analis virus dari

Ilustr

seba
cukup

"Dilih
seper
dilaku
detikI

Pun d
keheb
khusu
meng
tua ja

"Baga
ini ma
porno

Dijaba
denga

Game untuk Ponsel Pintar Disusupi Virus

Febrina Ayu Scottiati - detikinet

Jakarta - Para peretas rupanya telah menanamkan virus ke dalam game yang dirancang untuk ponsel pintar berbasis Windows. Diduga, mereka sengaja menargetkan pengguna

Dituding Bocorkan Data, FB Kebanjiran IkIan

Digugat membocorkan data pengguna, tapi sejumlah perusahaan makin suka beriklan di FB.

Indra Darmawan

(Silicon Alley Insider)

serta daftar

Menurut Go
Facebook n
saat ada pe
iklan. Jadi s
referrer he

BERITA TERKAIT

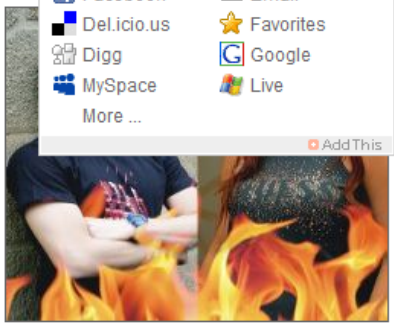
- Gara-Gara Facebook Gamer Zynga Merosot
- Facebook Tambahkan 'Related

Penjahat Cyber Mulai Dompleng 'Ariel Peterporn'

Kamis, 10 Juni 2010 - 13:18 wib

Susetyo Dwi Prihadi - Okezone

JAKARTA - Kabar yang menghembuskan kalau ada 23 video panas lainnya yang melibatkan Ariel dengan sejumlah artis mendapat perhatian serius. Apalagi setelah video yang mirip dengan musisi tersebut, beredar luas sebelumnya.



Ariel dan Aura Kasih (Foto: Iliketips)

Rasa keingintahuan yang besar membuat video lanjutan antara 'Ariel' yang kabarnya beradegan dengan artis Aura Kasih menjadi perbincangan hangat di sejumlah situs jejaring sosial, seperti Facebook, Twitter, dan lain sebagainya. Sialnya, panasnya isu ini dimanfaatkan oleh sejumlah orang tak bertanggung jawab.

Melalui Twitter, para penjahat cyber tersebut menjebak para pengguna Twitter yang lain, baik yang hanya sekedar iseng sampai yang memanfaatkan untuk tindakan yang membahayakan bagi pengguna mikroblogging tersebut.

Ditelusuri **okezone**, Kamis (10/6/2010), banyak link-link menjebak yang mengatakan kalau link tersebut adalah video lanjutan dari artis yang mirip dengan Ariel dan Aura Kasih. Namun sayangnya, saat di-klik link tersebut malah di-direct ke situs tertentu. Kuat dugaan ini dilakukan untuk menaikkan rating situs tersebut.

Yang iseng, link tersebut malah menampilkan sebuah gambat seperti nenek sihir yang sedang tertawa. Tak pelak, banyak orang yang tertipu dengan link tersebut.

ya
99
juta

ık.

langkah-
t lunak dan
Microsoft.

Arti "Keamanan Informasi"

- Proses terus-menerus melindungi aset-aset informasi digital
- Keamanan Informasi merupakan bagian dari Sistem, bukan sekedar fitur
- Tidak ada yang aman 100%
- Topik yang termasuk dalam Keamanan Informasi:
  - Kebijakan & Prosedur, Otentikasi, Cyber Attacks, Remote Access, E-mail, Website, Wireless, Devices, Media/Medium, Secure Architectures, IPSec, Sistem Operasi, Secure Code, Cryptography, Physical Security, Digital Media Analysis (Forensics), Audit, Integritas data dst

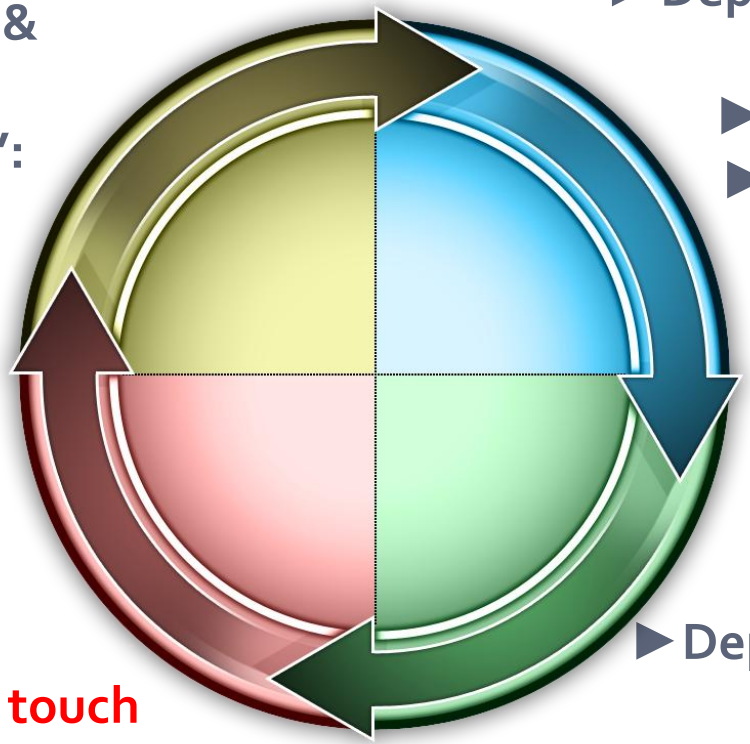
Information Security LiveCycle

Prevention

- Patch immediately (manage centrally)
- Keep passwords secret & change them regularly
- "Rule of least privilege": Control access to all your assets
- Apply proper coding & configuration practices

Protection

- Deploy "Defense-in-Depth"
  - Segregate networks
  - Tighten down firewalls
  - Be vigilant & stay alert



Response

- Do incident forensics
  - Leave "ON", disconnect & **don't touch**
- Recover…
- Analyze causes & apply lessons learned

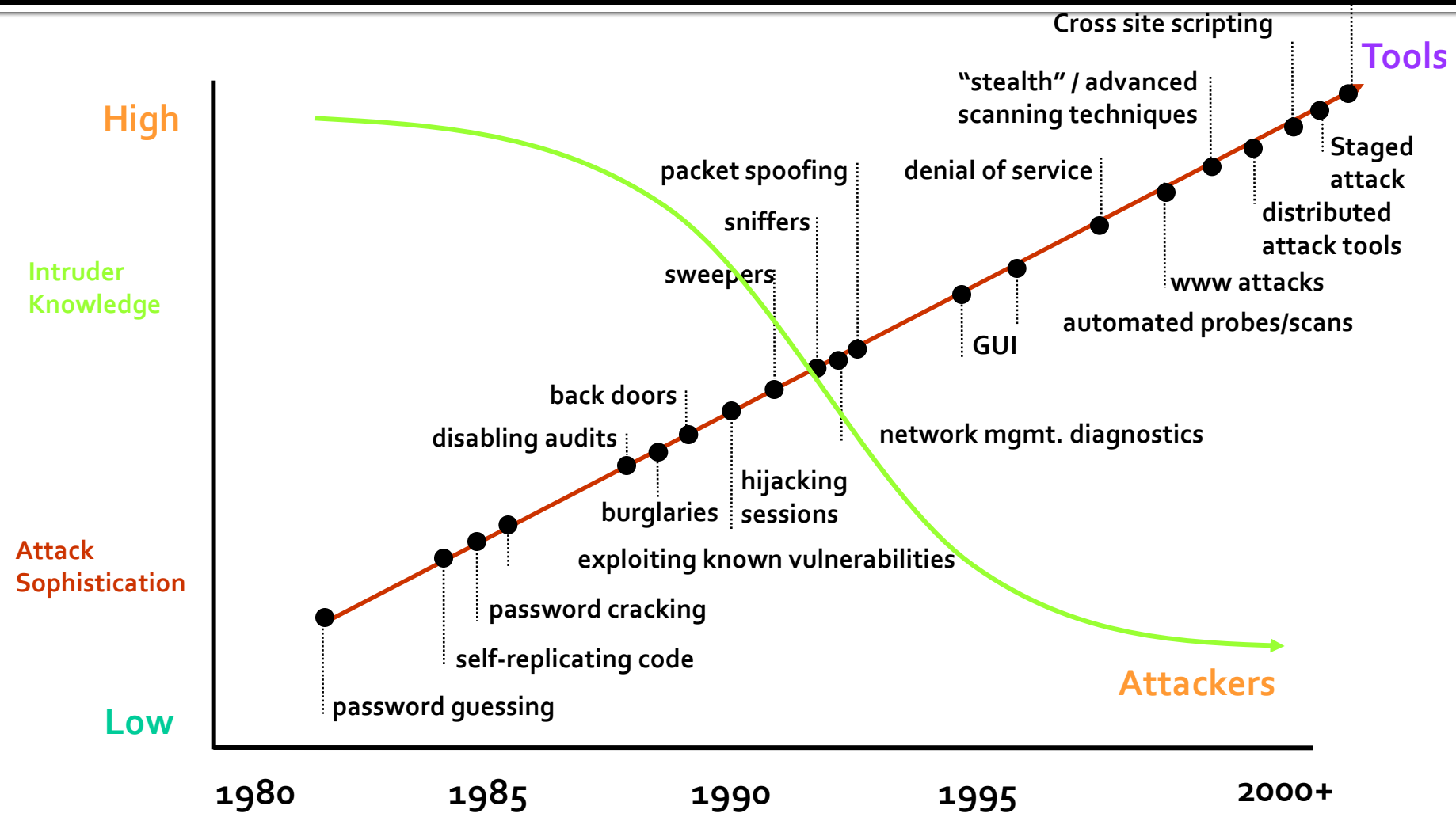
Detection

- Monitor traffic
- Deploy intrusion detection (host-, network-based)
- Maintain up-to-date anti-virus software
- Enable & monitor system logging
- Be vigilant & stay alert

Pentingnya "Keamanan Informasi"

- Mencegah Pencurian Data
- Menghindali konsekuensi legal dari tanpa melindungi informasi
- Menjaga produktivitas
- Mencegah dan mengantisipasi terjadinya cyberterrorism
- Menghindari penyalahgunaan identitas

Tantangan "Keamanan Informasi"-1



Evolusi Serangan Cyber

Source: CERT

Tantangan "Keamanan Informasi"-2

- Frekwensi dan jumlah serangan bertambah
- Jenis Serangan yang bertambah kompleks
- Deteksi kelemahan sistem semakin mudah dan cepat diketahui
- Serangan Terdistribusi
- Kesulitan dalam melakukan perbaikan (Patching)

Lapisan Keamanan Informasi

Umumnya orang-orang hanya terfokus pada bagian ini

Kutipan dari seorang Hacker

"People are the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."

- Kevin Mitnick-
disebut "God of Social Engineering"

Ancaman Cyber saat ini

- Pencurian dan Penyalahgunaan Identitas
- Malware
- Patch Management (Software Update/Patching)
- Denial of Services (DoS & DDoS)

Pencurian dan penyalahgunaan Identitas

- Penyalahgunaan Kartu Kredit orang lain oleh para Carder
- Takeover Account IM (Yahoo!, MSN, Google dll)
- Takeover Facebook, Twitter (Social Network)
- Teknik Phising digunakan untuk menjebak account tertentu dengan tujuan mendapatkan informasi financial pengguna

Contoh Mail Phising

From: "Ugm Technical Support Helpdesk" <alert@ugm.ac.id>
Sent: Sunday, March 14, 2010 10:42:27 PM
Subject: Dear Ugm.Ac.Id User

Attention Ugm.Ac.Id E-mail Account Holder,

Dear Ugm.Ac.Id User. All mailhub systems will undergo regularly scheduled maintenance, and access to your mailbox via our mail portal will be unavailable for some time during this maintenance period.

We shall be carrying out service maintenance/upgrade on our database and e-mail account center for better online services. We are also deleting all unused e-mail accounts to create more space for new accounts.In order to ensure you do not experience service interruptions or possible deactivation of your e-mail account, Please you must reply to this mail immediately confirming your e-mail account details below for confirmation and identification.

1. First Name & Last:
2. Full Login Email:
3. User Name:
4. Password:
5. Current Password:

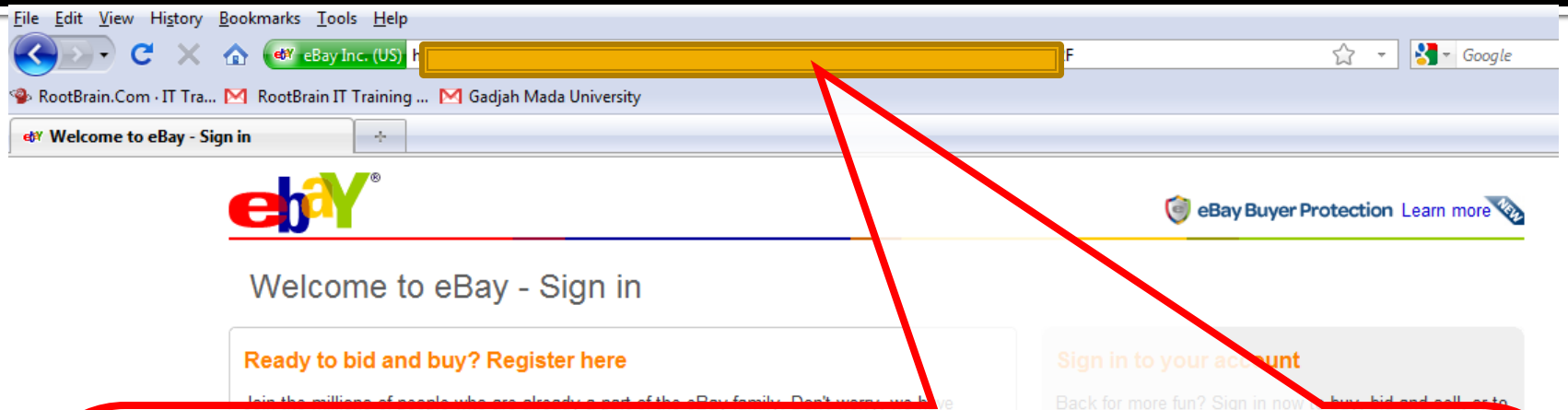
Failure to do this may automatically render your e-mail account deactivated from our e-mail database/mail server. To enable us upgrade your e-mail account, please do reply to this mail.

UGM Information
Technical Support
Account Management.

Alamat email pengirim dengan mudah dipalsukan!

Pahami metode serangan "Phishing" ini .
Admin tidak pernah meminta password dari user.

Phising URL



Pastikan mana URL Ebay yang benar ?

- http://www.ebay.com\cgi-bin\login?ds=1%204324@%31%33%37%2e%31%33%38%2e%31%33%37%2e%31%37%37/p?uh3f223d **[SALAH]**
- http://www.ebay.com/ws/eBayISAPI.dll?SignIn **[SALAH]**
- http://scgi.ebay.com/ws/eBayISAPI.dll?RegisterEnterInfo&siteid=0&co_partnerid=2&usage=0&ru=http%3A%2F%2Fwww.ebay.com&rafId=0&encRafId=default **[BENAR]**
- http://secure-ebay.com **[SALAH]**

Malicious Software (Malware)

- Software yang di disain agar bekerja tanpa izin atau tidak diketahui oleh user
- Dapat merubah atau merusak data
- Dapat mengoperasikan perangkat keras tanpa otorisasi
- Dapat mengambil alih proses yang dilakukan oleh Web browser
- Mampu mencuri informasi penting/confidential lainnya dari komputer pengguna

Jenis Malware

- Virus
- Worm
- Spyware
- Keyloggers
- Rootkits
- Mobile malware

Virus

- Program komputer yang dapat mereplikasikan diri sendiri dan menyebar melalui jaringan melalui file sharing, email, adware, file PDF, Doc dll dengan bantuan pengguna
- Virus biasanya dapat merusak data, file system serta konfigurasi

Worm

- Program Komputer yang dapat mereplikasikan diri melalui jaringan tanpa bantuan pengguna.
- Worm ini selain merusak aplikasi umumnya juga menggangu performa jaringan atau bahkan melakukan DoS (Denial of Services) terhadap server atau jaringan

Spyware

- Program mata-mata yang digunakan oleh hacker untuk mendapatkan informasi yang diinginkan dari seseorang.
- Spyware sering berupa advertisement (iklan) yang menggoda user untuk memasang/mengklik/membuka/ mengeksekusi software tertentu. Popups yang tidak terkontrol sering menjadi tanda terinfeksi.

Keylogger

- Program spyware yang secara khusus digunakan untuk merekam keystroke pada keyboard atau bahkan mampu menyimpan tampilan screen sebuah computer
- Keylogger ada yang berupa software dan hardware

RootKit

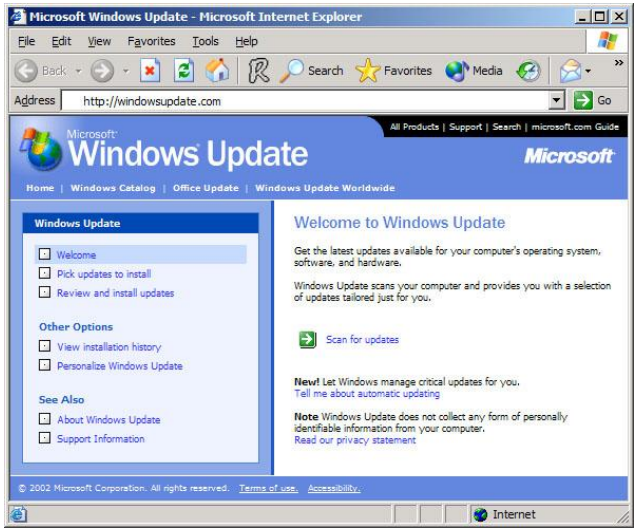
- Kumpulan Program yang dapat digunakan untuk memanipulasi proses berjalan, file system atau aplikasi data dengan tujuan membantu penyusup untuk maintain akses system tanpa terdeteksi.
- Banyak jenis RootKit tersedia pada setiap OS
- Sulit dideteksi

Mobile Malware

- Saat ini banyak sekali virus, trojan, dan worm yang menginfeksi perangkat mobile spt Handphone dan SmartPhone.
- Malware di mobile ini umumnya menyebar dari Aplikasi Ilegal di internet, Bluetooth dan SMS/MMS.

Patch Management tidak dilakukan

- Patch Management : menginstall Software Update atau Patching, untuk menutup bugs yang ditemukan.
- 90% serangan cyber berhasil diakibatkan keteledoran administrator tidak segera melakukan update/patching ketika suatu bugs ditemukan.
- Bugs dapat diexploitasi oleh hacker.



Security Tools Best Practices

- Anti-virus software
- Anti-spyware software
- Windows and applications updates
- Security bundles
- Personal firewalls
- Wireless
- Other best practices

Anti-virus Software

- McAfee: Virus Scan
- Symantec: Norton Anti-Virus
- Computer Associates: eTrust EZ AntiVirus
- Trend Micro: PC-cillian
- Grisoft: AVG Anti-Virus (**freeware**)
- Alwil Software: Avast! AntiVirus (**freeware**)
- eset: NOD32 (**freeware**)
- Clamav

AntiSpyware

- Sunbelt Software: CounterSpy
- Webroot Software: Spy Sweeper
- Trend Micro: Anti-Spyware
- HijackThis (**freeware**)
- Lavasoft: Ad-Aware SE Personal (**freeware**)
- Spybot: Search & Destroy (**freeware**)
- Microsoft: Windows Defender (**freeware**)

Security Bundle Tools

- McAfee: Internet Security Suite
- Symantec: Norton Internet Security
- Computer Associates: eTrust EZ Armor
- Trend Micro: PC-cillian Internet Security
- ZoneAlarm: Internet Security Suite
- F-Secure: Internet Security
- MicroWorld: eScan Internet Security Suite
- Panda Software: Panda Internet Security
- Softwin BitDefender Professional Edition
- eXtendia Security Suite
- Clamav/Amavisd

Personal Firewall Programs

- Zone Labs
- Symantec's Norton Personal Firewall
- Sunbelt's Kerio Personal Firewall
- Tiny Software's Tiny Personal Firewall
- Mac OS X
- Windows XP (with Service Pack 2 & 3)
- Windows Vista & 7 (Seven)
- Linux OS (ufw/shorewall/iptables)

Step Best Practices Security

1. Install OS/Software Updates

2. Run Anti-virus Software

3. Prevent Identity Theft

4. Turn on Personal Firewalls

5. Avoid Spyware/Adware

6. Protect Passwords

7. Back up Important Files