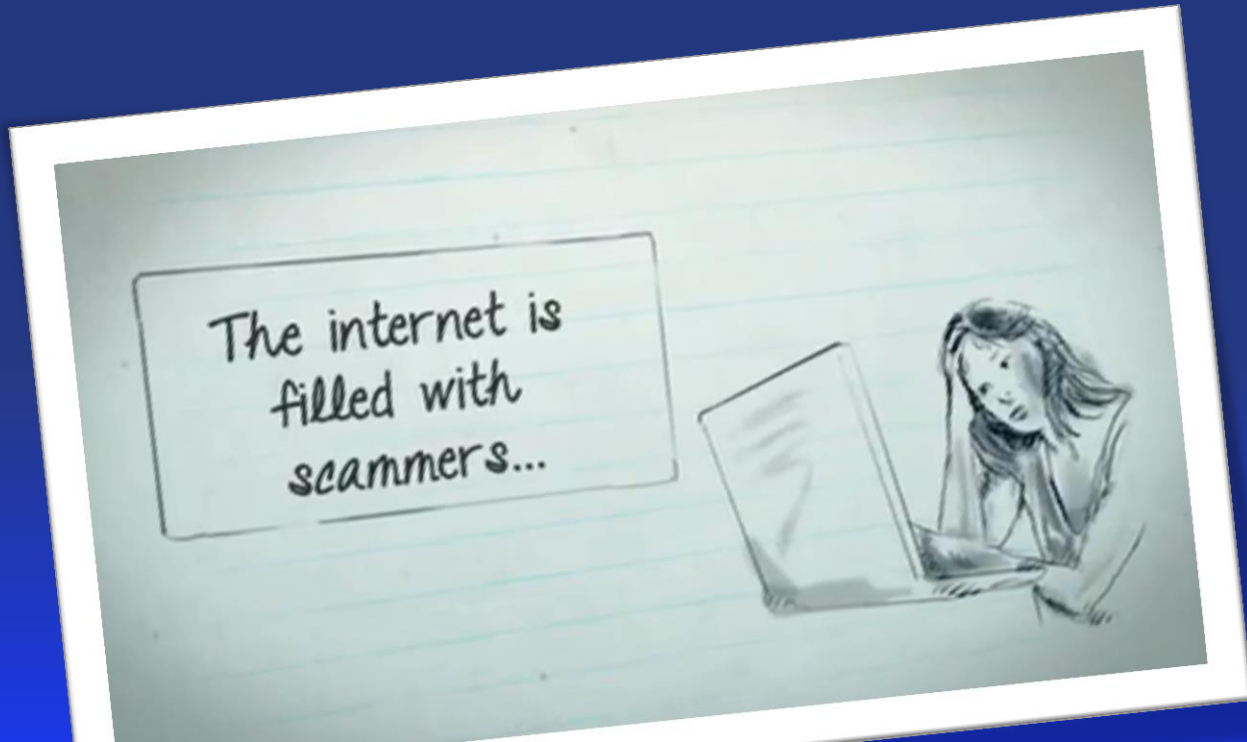


Cyber Crime Seminar



No Victim Too Small – Why Small Businesses Are Low Hanging Fruit



Why Are We Here?



- What is Cybercrime?
- Why YOU may become the next victim?
- What do they attack?
- Why do they attack?
- How to protect yourself, your family, and your business!

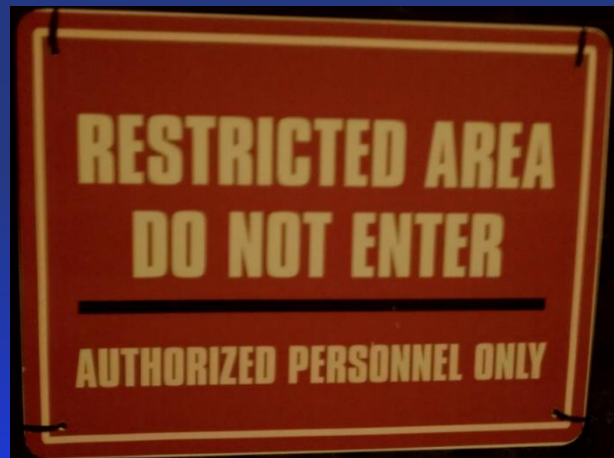


Why This Is Important ~ A Little History



- 289,874 is the number of REPORTED incidents in 2012
- \$525,441,110 is the amount of REPORTED funds stolen in 2012

Hackers Don't Have Rules, Regulations And Don't
Have To Meet Compliance Concerns Like HIPAA,
HiTech, PCI, Sarbanes Oxley, Basel III, Etc...





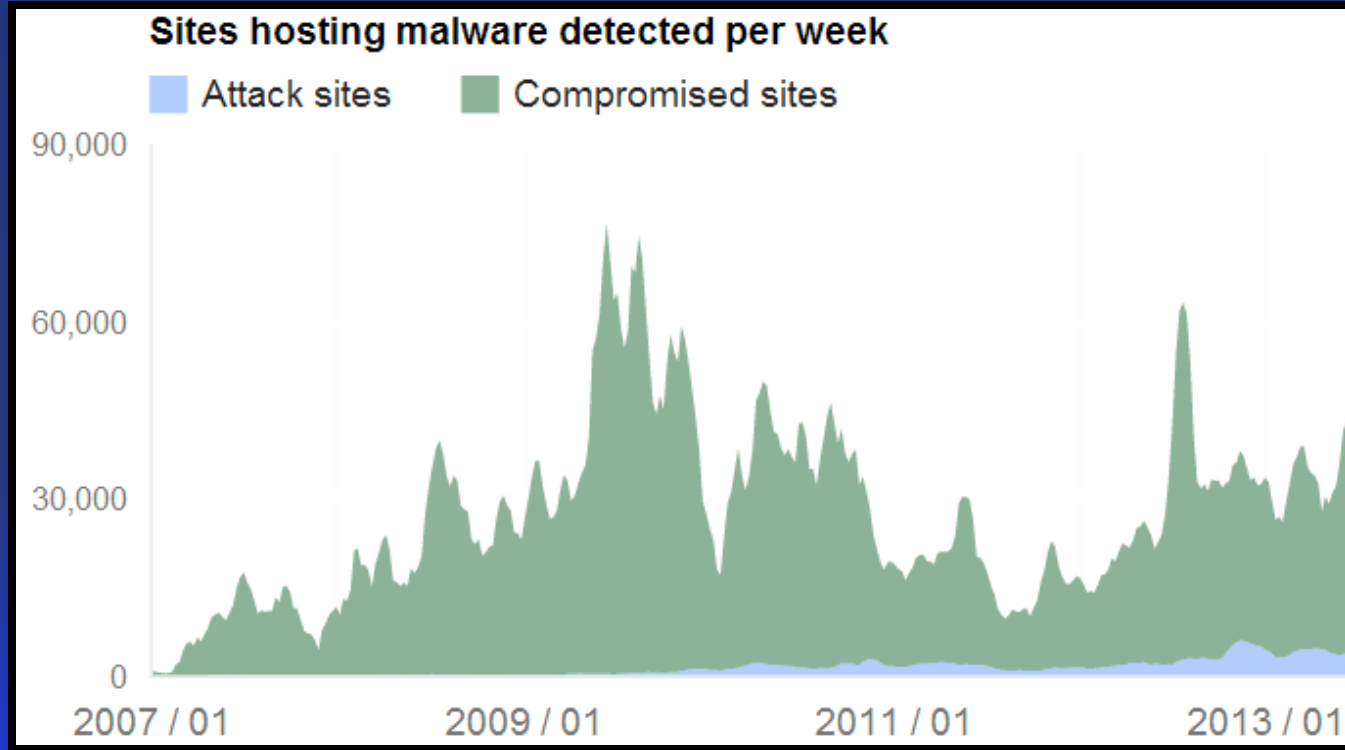
Common PC Rationales?

- There's Nothing A Hacker Would Want On My PC.
- I Don't Store Sensitive Information On My PC.
- I Only Use It For Checking E-mail.
- My Company Isn't Big Enough To Worry About Hackers?

How Valuable Is A Hacked Workstation



Waves of Attacks



What An Attack Might Look Like



The image displays two overlapping security software interfaces. The background window is 'Internet Security 2010', showing a 'System Scan' in progress. The scan type is set to 'Quick'. The results table lists several threats detected on the C:\WINDOWS\... drive.

#	Vendor	Type	Location	Threat level	Description
1	Trojan-Clicker...	Trojan Programs	C:\WINDOWS\...	Low Risk	This Trojan...
2	Virus:W32/Alma...	Replicating	C:\WINDOWS\...	Low risk	A program...
3	Trojan-Dropper...	Trojan Programs	C:\WINDOWS\...	Middle Risk	This Trojan...
4	Email-Worm.Wi...	Network Worms	C:\WINDOWS\...	High Risk	This worm...
5	Trojan-Spy.HT...	Trojan Programs	C:\WINDOWS\...	High Risk	This Trojan...
6	Trojan:W32/Pa...	Trojan	C:\WINDOWS\...	High risk	A Trojan horse...
7	Email-Worm.BA...	Network Worms	C:\WINDOWS\...	High Risk	This worm...
8	Trojan:Downloader...	Trojan Programs	C:\WINDOWS\...	Middle Risk	This Trojan...

Below the table, it shows 'Objects scanned: 3828', 'Threats detected: 25', 'Fixed: 0', and 'Removed: 0'. A 'TRIAL VERSION' watermark is visible.

The foreground window is 'Windows Advanced Security Center'. It shows a 'Warning! Your computer is at risk!' message. The 'Security Essentials' section indicates that 'FireWall', 'Automatic updates', and 'Antivirus protection' are all turned 'Off'. The 'Status' section shows the last scan was on 8/9/2012 at 19:39:54, and the last update was on 8/9/2012 at 19:38:42. The database version is 1289. The 'Anti-phishing protection' and 'Advanced Process Control' are both 'Disabled'.



FBI Online Agent has blocked your computer for security reason

The work of your computer has been suspended on the grounds of unauthorized cyberactivity.

Described below are possible violations, you have made:

Article 274 – Copyright

A fine or imprisonment for the term of up to 4 years. (The use or sharing of copyrighted files – movies, software)

Article 183 – Pornography

A fine or imprisonment for the term of up to 2 years. (The use or distribution of pornographic files)

Article 184 – Pornography involving children (under 18 years)

Imprisonment for the term of up to 15 years. (The use or distribution of pornographic files)

Article 104 – Promoting Terrorism

Imprisonment for the term of up to 25 years. (You have visited websites of terrorist organizations)

Article 297 – Neglect computer use, entailing serious consequences

A fine or imprisonment for the term of up to 2 years. (Your computer has been infected with a virus, which, in turn, infected other computers)

In connection with the decision of the Government as of August 22, all of the violations described above could be considered as conditional in case of payment of a fine.

Amount of the fine is \$200. Payment must be made within 24 hours after the discovery of the violation. If the fine has not been paid, you will become the subject of criminal prosecution.

After paying the fine your computer will be unblocked

Case # 14670

Tracking time: 15 days 7 hours 17 min

Responsible agent: Charity Barker

Address: FBI Headquarters in Washington, D.C.

Detected items

- ✗ c:/tmp/Porno.avi
- ✗ c:/tmp/CH99823.avi
- ✗ c:/Program Files/gporno/DSC0065.JPG
- ✗ d:/photos/DSC0090.JPG
- ✗ c:/tmp/My_sex156.avi
- ✗ c:/windows/tmp/DSC00564.JPG
- ✗ c:/windows/system32/DSC2094.JPG



To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of **\$200**.



Exchange your cash for a MoneyPak voucher and use your voucher code in form below.

Please note: This fine may only be paid within 48 hours, if you let 48 hours pass without payment, the possibility of unlocking your computer expires.

In this case a criminal case against you will be initiated automatically.



Where can I buy MoneyPak



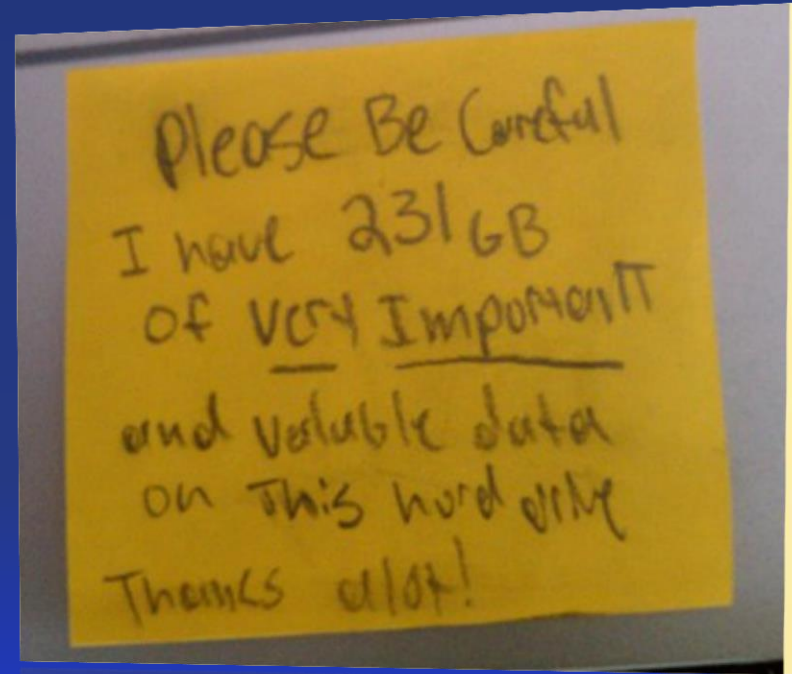
100%
Secure Payments

OK



Helpful Tip #1: Backup Your Data

1. Run Daily Backups of Critical Data
2. Automated Offsite Backups Are Invaluable
3. Check / Test Your Data Backups Monthly (Minimum)



Why Else Do They Want Your Workstation



\$28.90

What is your account worth to attackers?

\$28.90

What can I do to be safer?

- Use [Cloudsweeper](#) to find passwords already in your email account and redact or encrypt them.
- Change passwords that you've used at insecure sites, and consider using a [password manager](#) to assist you in using a different password for different sites.
- Safeguard access to your primary email account as best you can. Consider using [two factor authentication](#) - this setting makes it MUCH harder for an attacker to gain access to your account. You can enable two factor authentication on your google account [here](#).


Plain Text Passwords

These accounts send your password to you in plain text. If someone got access to your email account, they would be able to see the password you used for these accounts.

 [grammarly.com](#)

Email Password Resets

These accounts allow you to reset your account password with just access to your email account. If someone gained access to your email account, they would be able to access all of these accounts on your behalf.

 [Skype*](#)

 [Hulu *](#)

 [UPlay *](#)

 [Groupon](#)

 [Newegg](#)

Email Access+

These accounts provide or require additional information to prove your identity beyond access to your email account. If someone gained access to your email account, they would need extra information to access these accounts.

 [Twitter](#)

\$0.30

 [Google](#)

 [Facebook](#)

\$5.00

How They Get Paid

BlackHatStore.ru

My account

Forum

chat LIVE SUPPORT
offline

Hello, crack3d! You have 0 credits

blackhat

Help | Replacements

Dashboard

Order history

Buy credits

Transfer credits

Replacement policy

Sign Out

For Replacements and CREDIT PROBLEMS create a ticket by clicking "Help | Replacements" - Our staff will respond as ap to your problems



Country	Extra	Price
United States	Mystery Shopper Result	1.00
United States	Mystery Shopper Result	1.00
United States	Mystery Shopper Result	1.00
United States	Mystery Shopper Result	1.00

PayPal Checker

pp checker [c] cyber [ICQ: 33333353]

PayPal Accounts List (acc:pass)

Socks List (server:port) Socks5

Check

Options < <

Options

☒ Don't check with passwords < 8 dig

☒ Check credit cards attached

☒ Check bank accounts attached

☐ Check address

☐ Check primary e-mail

☐ Check phone number

☐ Check last transaction info

☐ Check Instant (800-9005) BETA!!!

☐ Check Limits

☐ Result in linear mode

☐ Show User-agent in result file

☐ Check Socks in BlackList

☐ Load Socks List from URL

Accs: 0 Socks: 0

Valid: 0 Looked: 0

Invalid: 0 Errors: 0

Security Measures: 0

Upd. Security Questions: 0

Security Code: 0

Facebook Checker

Account Info

Accounts List

C:\Delphi\Checkers\Facebook

Socks List (ip:port)

C:\Delphi\Checkers\Facebook

Check

Accs: 0

Valid: 4

Threads: 2

Invalid: 9

Status: Ended. Stopped

Amazon Checker

Accounts information

Accounts List

Threads: 1

Socks List

Check

Accs: 0

Valid: 0

Socks: 0

Invalid: 0

Status: Stopped

Amex Checker

Billing Info

CC List

Socks List

Check

CC: 0

Can enroll: 0

Socks: 0

Enrolled: 0

Status: Stopped

Apple iTunes CC Checker

Billing Info

CC List

Socks List

Check

Skype Accs. Checker

Free Skype Accounts Checker

Accounts List (acc:password)

Socks List (ip:port)

Check

Threads: 1

Autosave: 5

☐ HTTP(S) ☐ Socks4 ☒ Socks5

Accounts: 0

Valid: 0

Socks: 0

Errors: 0

Status: Stopped

eBay Checker

Billing Info

Accounts List

Socks List (server:port) Socks5

Check

Accs: 0

Valid: 0

Socks: 0

Invalid: 0

Status: Stopped

Walmart Checker

Info

Accounts list

Socks List (ip:port)

Check

Accs: 0

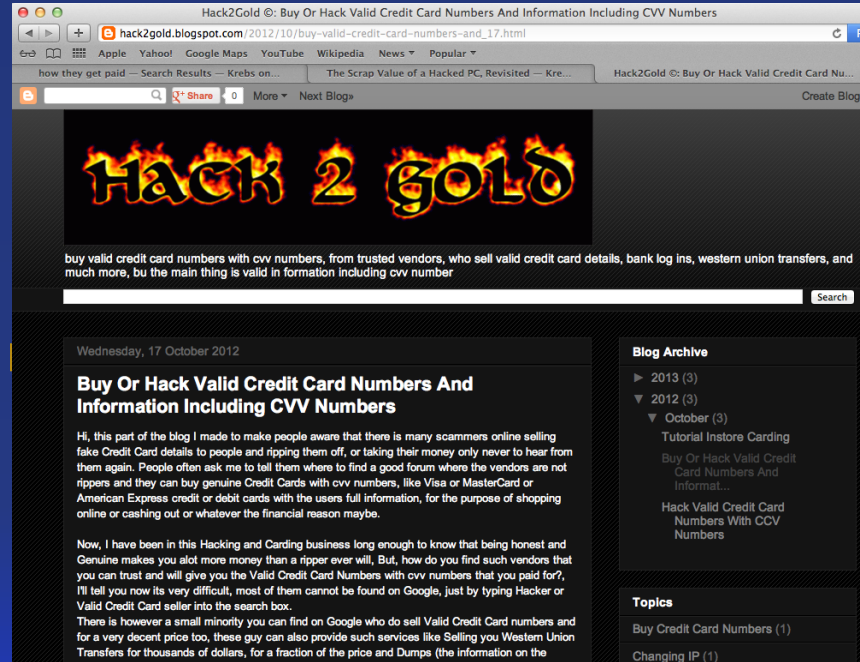
Valid: 0

Alertpay Checker

PM Mail Checker

MB Checker

What Does It Look Like



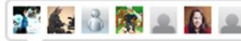
Real Value?

One prominent credential seller in the underground reported:

- **iTunes** accounts for \$8
- **Fedex.com**, **Continental.com** and **United.com** accounts for USD \$6
- **Groupon.com** accounts fetch \$5
- \$4 buys hacked credentials at registrar and hosting provider **Godaddy.com**, as well as wireless providers **Att.com**, **Sprint.com**, **Verizonwireless.com**, and **Tmobile.com**
- Active accounts at **Facebook** and **Twitter** retail for just \$2.50 each

TECH | 7/21/2013 @ 9:31AM | 344,691 views

SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phones



39 comments, 16 called-out

+ Comment Now

+ Follow Comments



Security researcher Karsten Nohl says some SIM cards can be compromised because of wrongly configured Java Card software and weak encryption keys; Photo credit Luca

93% of companies that lose their data - file for bankruptcy within 1 year [National Archives]



“3D Printing And Credit Card Skimmers!”



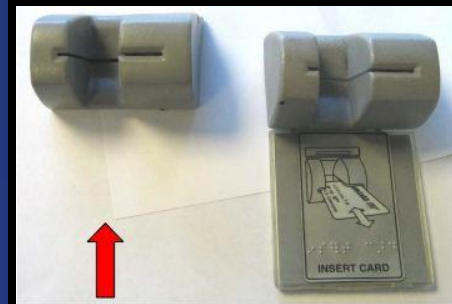
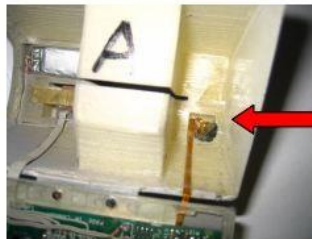
This is the back side of the device.

The card reader is on the left and the camera is tucked into the right side as shown below.

The device may have been constructed with parts from an MP3 Player.

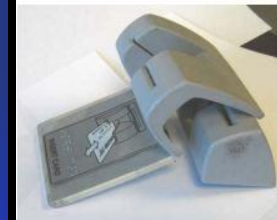
It was attached with several small pieces grey double-sided tape

The part was well made and fit nicely over the original card reader.



The real card reader slot.

The capture device



The side cut out is not visible when on the ATM.



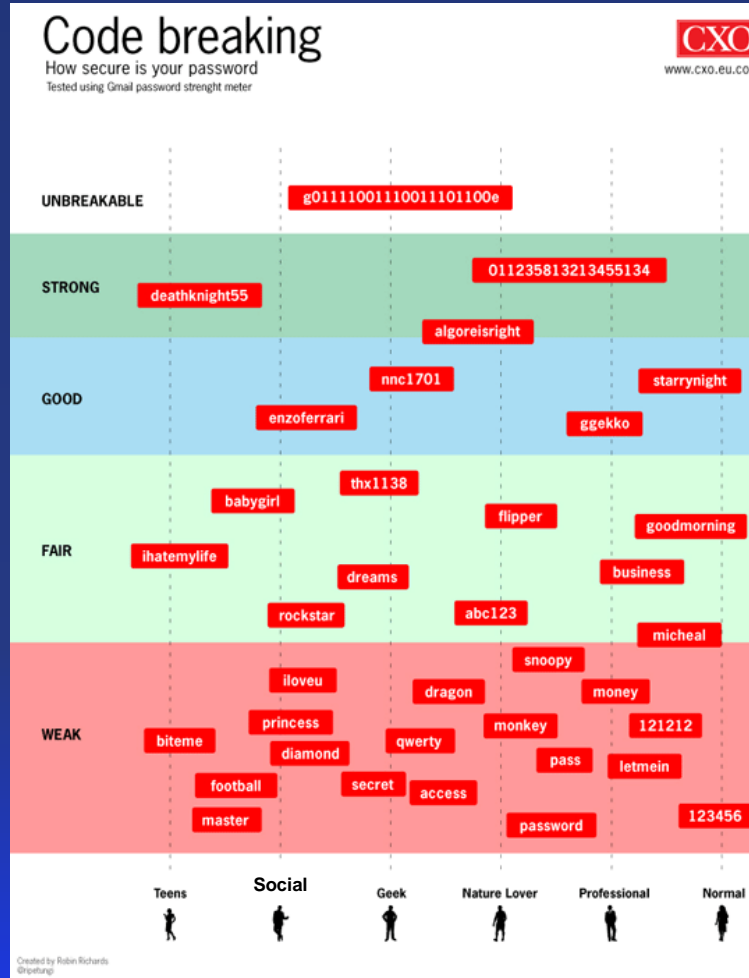
Helpful Tip #2: Multiple Bank Accounts



1. One Account for Payroll and Taxes
 - NO DEBIT OR CREDIT CARDS ASSOCIATED WITH THIS ACCOUNT
2. One Account for Operations & Expenses
 - AVOID DEBIT OR CREDIT CARDS ASSOCIATED WITH THIS ACCOUNT



Password Examples





Helpful Tip #3: Password Rules

1. DON'T SHARE PASSWORDS
 - This includes your “IT Guy”
 - Type your password for them
2. One Password Per Account
3. No Password POST-IT NOTES!
4. Change Your Password Every 60 Days
5. Use a phrase with numbers and characters:
“I Only Have Eyes For You”

→ “!0hE4uAug”

And here's the list of the 10 most hacked passwords of hacked Yahoo! accounts, according to ESET.

1. '123456' used by 1666 (0.38%)
2. 'password' used by 780 (0.18%)
3. 'welcome' used by 436 (0.1%)
4. 'ninja' used by 333 (0.08%)
5. 'abc123' used by 250 (0.06%)
6. '123456789' used by 222 (0.05%)
7. '12345678' used by 208 (0.05%)
8. 'sunshine' used by 205 (0.05%)
9. 'princess' used by 202 (0.05%)
10. 'qwerty' used by 172 (0.04%)

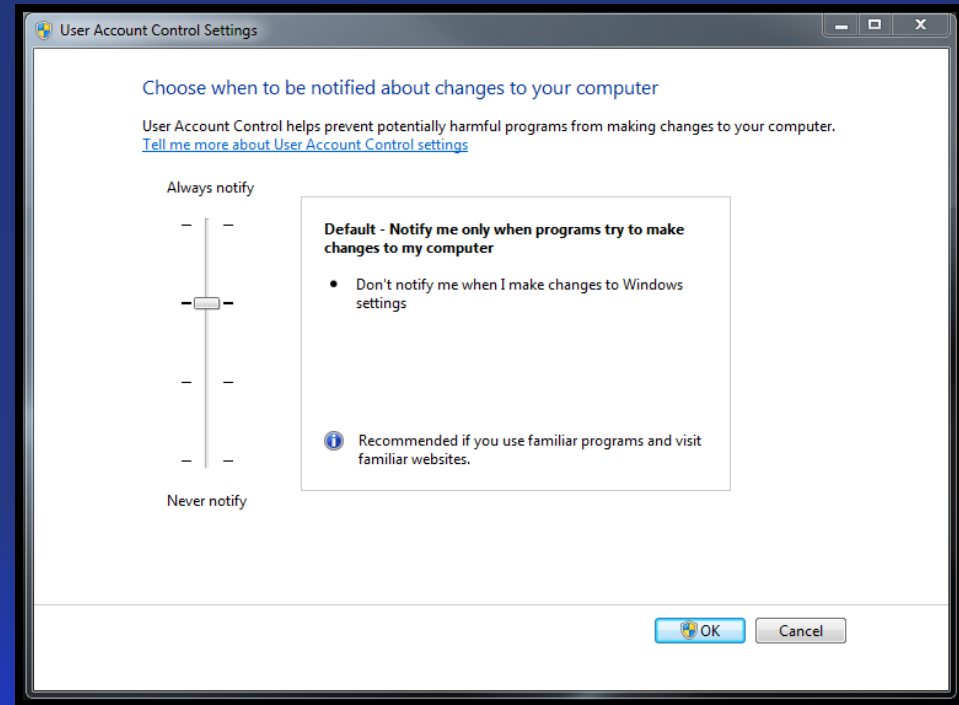


Helpful Tip #4: Windows Firewall & UAC

1. Re-Enable Windows Firewall
2. Install Current AntiVirus Software
(and keep it current please)
3. Enable User Access Control (UAC)

-- We know it is considered obnoxious,
but it really does work to help prevent
attacks against your workstation

>> Control Panel> User Accounts
4. Seek professional help to secure your
business network



Who Is Hacking: Why Are They Doing This



1. Chinese Army
Tied To Hacking US Companies
~ Better Natural Gas Prices
2. Russian Company Espionage
~ Caused A Competitor To Lose
Millions In Sales By Shutting
Them Down For A Week
3. Ukraine Hackers Steal Debit
Cards ~ Withdraw Millions From
Various New York ATM's
4. Nigerian Scams, And On, And
On...



Helpful Tip #5: What To Do If Attacked

1. Disconnect Your Workstation From The Network AND Internet
2. Seek Professional Help
3. When Appropriate, Contact The Police And Your Insurance Company
4. Don't Start "Googling" For The Fix
 - Russian firm w/ 500 employees wrote the bug and charged \$79.95 to your credit card to fix the solution they created in the first place!



Olvis Rafael Rodriguez, left, and Emir Yasser Yeje pose with bundles of cash allegedly stolen using bogus magnetic stripe cards at cash machines throughout New York. Photo: United States Attorney's Office for the Southern District of New York

Helpful Tip #6: Work Smarter

1. Name
2. Address
3. Phone
4. DOB
5. Education (College/High School)
6. Mother's Maiden Name?
7. Mothers fathers name
8. Friends names
9. Children's names
10. Children's school
11. Children's DOB
12. Pets name
13. Browsing habits (websites, services, hobbies, likes, etc...)
14. And on, and on and on...)



Social Media Policies and Procedures

1. Know who is authorized to add content
2. Type of content allowed
3. Who has access
4. Who has login info
5. Which sites are used
6. Employee Termination Policy



According to a Microsoft study, phishing via social Networks grew from 8.3% in 2010 to 84.5% in 2011 (increasing steadily since then)

B.Y.O.D.

(Bring Your Own Device)



If You Allow Users To Access

- Corporate E-mail
- Corporate Data
- Remote Access To Corp Network

Then You **MUST** have Mobile Device Management To Ensure You Can Wipe Your Corporate Data If The Device Is Lost Or Stolen.



N.Y.P.D. Has Setup An iPhone Unit

San Francisco ½ Of Crimes Reported Are Phone Theft

Where Do Employees Leave Your Corporate Data And Email?

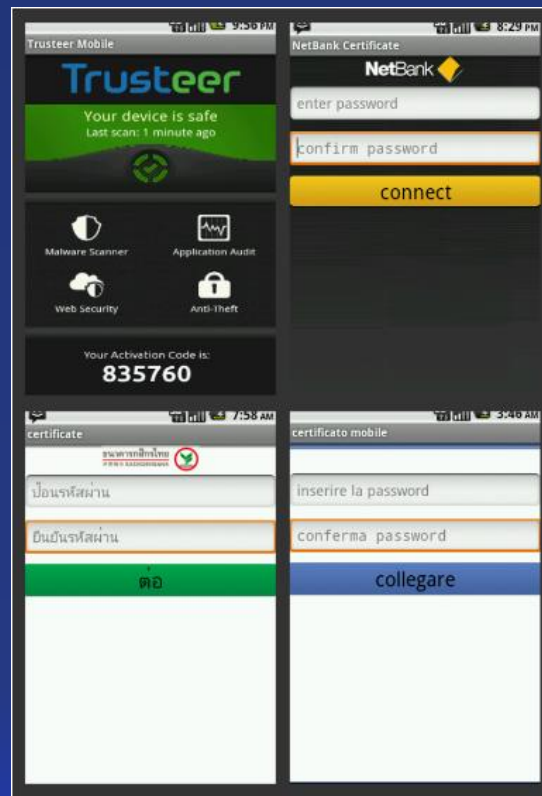


Put A
Lock
On Your
Phone

TODAY!

Perkele: Android Malware Kit

1. Can Help Defeat Multi-factor Authentication Used By Many Banks
2. Interacts With A Wide Variety Of Malware Already Resident On A Victim's PC
3. When A Victim Visits His Bank's Web Site, The Trojan Injects Malicious Code Prompting The User To Enter His Mobile Information, Including Phone Number And OS Type



When the bank sends an SMS with a one-time code, Perkele intercepts that code and sends it to the attacker's control server. Then the malicious script completes an unauthorized transaction.



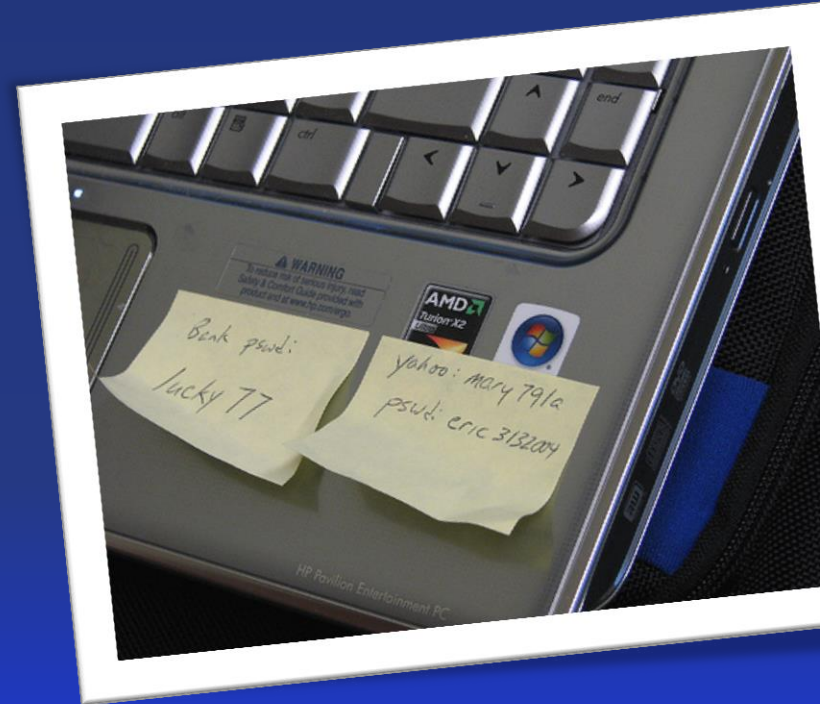
Helpful Tip #7: Common Sense Security

- Train Staff On Social Engineering!
- Know The Source
- Limit Telephone Information Sharing
- Physical Security
- Wireless “Hot Spots” & Hotel Internet
- Your Equipment @ Offsite Locations including Starbucks & Conferences
- Ability To Disable The Device If It's Lost Or Stolen (LoJack, Encryption, Etc.)

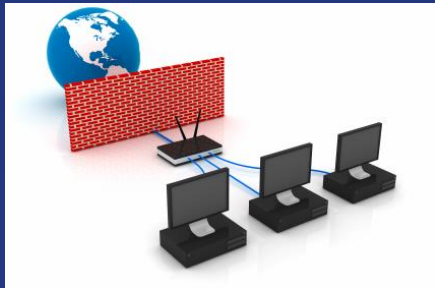


Helpful Tip #8: Advanced Security Tips

- Don't Use "Home" Version of Microsoft Windows On Your Company Workstations
- Encrypt Your Hard Drive
- Use Email Hygiene Provider / Service
- Use Server Based Group Policies
- Use MSP to Manage Company Firewall(s)
- Establish Company-wide Data Policies



All You Needed In The 90's



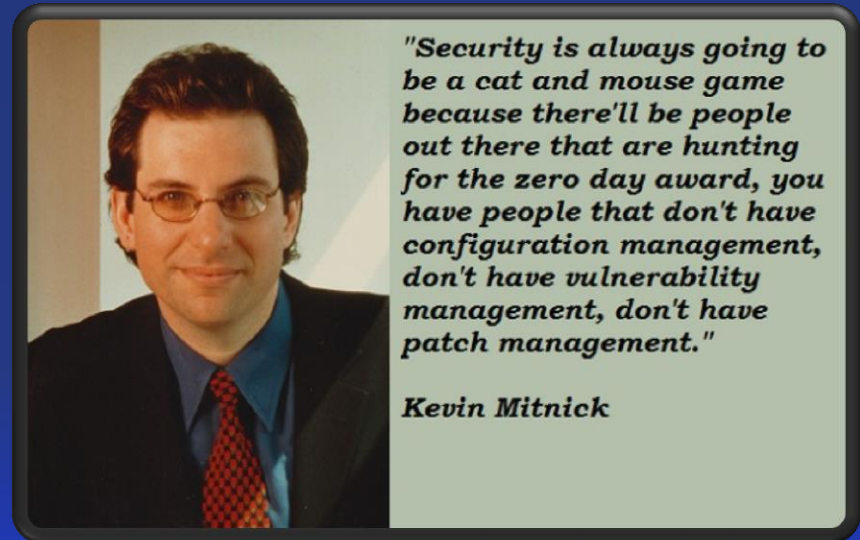
- Basic Firewall
- Antivirus
- Tape Backup
- A Good Mullet



Mullets! Mullets! Mullets!

Helpful Tip #9: Patches, Updates, & Your Network

- Review & Test Your Backups
- Patch Management
- Force Password Changes
- Implement Password Policies
- Secure ALL Mobile Devices
- Review Workstation Security
- Review Network Security
- Enforce Content Filtering



What's Next on Cybercriminals Agenda?

1. Website Accounts: Twitter, Facebook, Pinterest, YOUR WEBSITE
2. Home Automation Systems
3. Video Conferencing Systems
4. Video Surveillance Systems
5. Refrigerator and Other Network Appliances
6. HVAC Systems (U.S. Chamber of Commerce)
7. Automobiles, Phones, & Televisions

**** Recent Paid Test Results In Disabled Brakes****

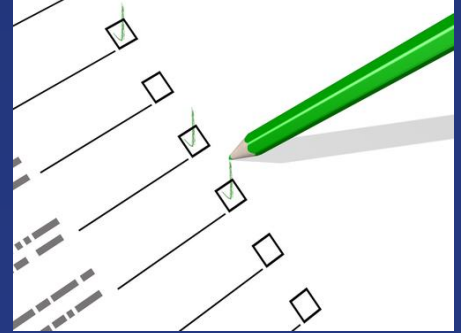


What's Next on YOUR Agenda? *Network Security Audit*



1. Fill Out The Audit Contact Form
2. Business Development Will Schedule An On-site Pre-Audit Meeting
3. Engineer Will Be Scheduled For On-site Visit
4. Engineer and Business Development Will Discuss The Findings Of The Audit
5. Follow Up Client Meeting To Discuss Recommendations And Findings Of The Audit

~~\$1995~~

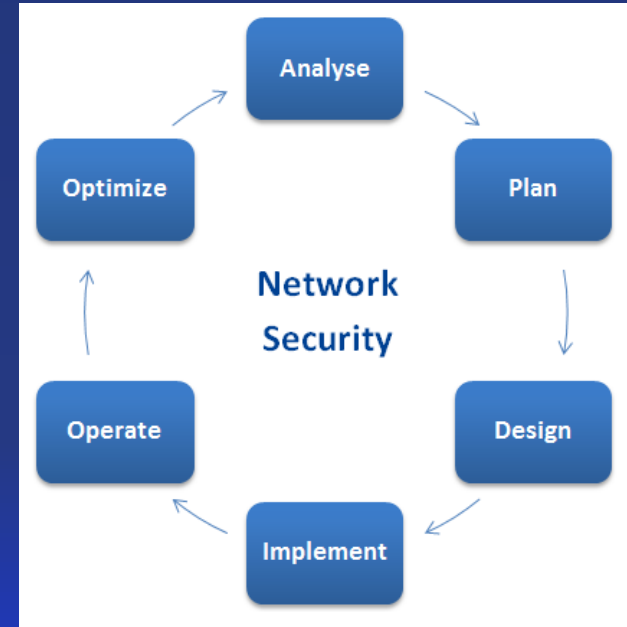


**\$995 Today
Only**

What Happens Next? One of Two Things Happens



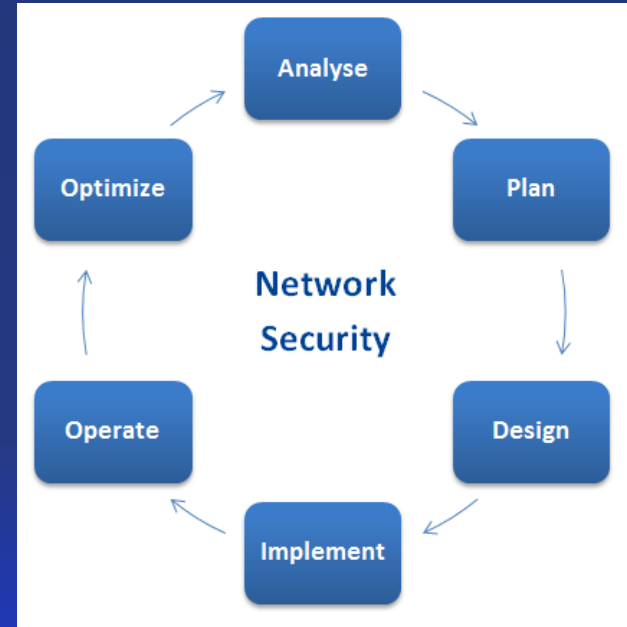
1. You love the plan but decide to implement it on **your own**. *If this is the case, we'll wish you the best of luck and ask that you keep in touch with us to let us know how you're doing*



What Happens Next? One of Two Things Happens



2. You love the plan and ask us to get you protected **ASAP**. *If that's the case, we'll knock it out of the park ... and that's a promise.*



About Nashville Computer



Founded 1988

NashvilleComputer.com 615-377-0054



- 16 Employees On Staff
- 4 Full Time Helpdesk Engineers
- 4 Full Time Senior Level Engineers
- Customized IT Solutions To Fit Your Business
- Website Design And Hosting

