



Social Engineering & Security Primer

AKA "People are bastard
covered bastards with
bastard-filling."

Hacking, Cracking, Phishing, Zombies – OMGWTFSRSLY?

- **Hacker:** someone who breaks into computer networks for legitimate or illegitimate reasons. (This definition has changed over time and still means a few different things.)
- **Cracker:** someone who reverse-engineers computer software for the purpose of embedding spyware/malware or working around commercial licenses ("Warez").
- **Phishing:** attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.



WARNING!

The word "hacker" does not inherently imply illegal or unethical behavior. The negative connotation came years later, as "hacker" originated as a positive term for people who kick ass at computers and/or coding.

Hackers get very upset when this word is misused.
Very. Upset.



Malicious Hacking Has Grown Up

- Years ago, hacking was often done for just fun and bragging rights.
- Today, hacking is a lucrative industry often backed by organized crime.
- LOTS of \$\$\$ to be made stealing identities, credit card info, etc.



Why Hackers Hack

- To steal/sell identities, credit card numbers, corporate secrets, military secrets
- Fun, Excitement and/or Notoriety
- Political ("Hacktivism")
- Revenge
- Blackhat SEO



White Hat vs Black Hat

White Hat: The Good Guys.

Grey Hat: The (Mostly) Good
Guys

Black Hat: The Bad Guys

This is over-simplified, of
course, but you get the
gist,

Virus

Self-replicating program that infects a system without authorization.

They can install keyloggers, download, delete or alter files, render a system unusable or worse.

Travels from computer to computer.

(No, they cannot spread to humans. Yet.)





Worm

Similar to a virus, but can self-replicate without human interaction.

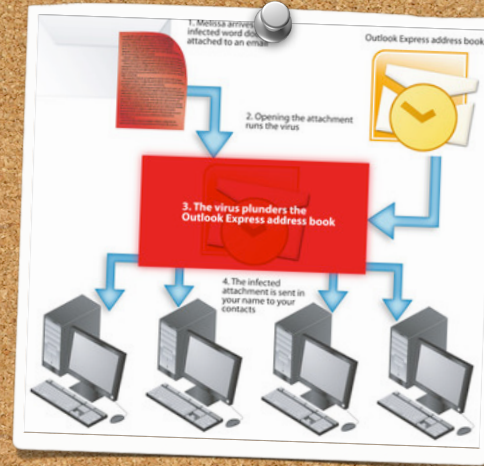
Takes advantage of network transport protocols - can send thousands of copies of itself.

Worm Example

A worm sends a copy of itself to everyone in your e-mail address book.

The worm then replicates and sends itself out to everyone listed in each of the recipient's address book.

And so on, and so on.

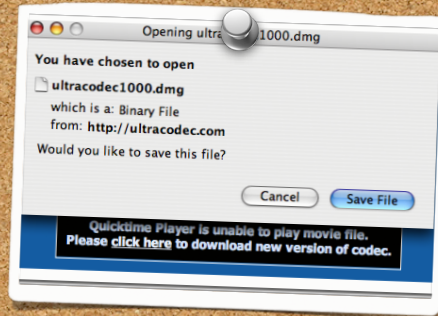




Trojan Horse

Masquerades as useful software such as anti-virus, video codecs, browser plugins, etc.

Victims are tricked into opening Trojan Horse files because they appear to be receiving legitimate software or files from a legitimate source.



**Macs are NOT
Immune**

**Trojans frequently appear as
fake video codec downloads,
rogue anti-virus
("scareware"), and
attachments in emails such
as phony receipts.**



Email Attachments

Spooled emails that contain malware attachments frequently appear to come from Amazon.Com, PayPal, E-Bay, iTunes, and Banks.

They often use the scare tactic that the recipient's account has been suspended or compromised.

Your account has been temporarily limited! From: PayPal <updates-int@paypal.net>
Subject: Your account has been temporarily limited!
From: PayPal <updates-int@paypal.net>
Date: 2011-01-07 06:02:23

Dear PayPal account holder,

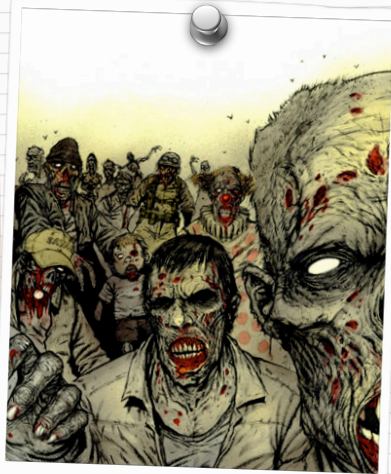
PayPal is constantly working to ensure security by regularly screening the accounts in our system. We have recently determined that different computers have tried logging into your PayPal account, and multiple password failures were present before the logons.

Until we can collect secure information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.

Download and fill out the form to resolve the problem and then log into your account.

Thanks ,
PayPal

Botnets (AKA "Zombie Armies")



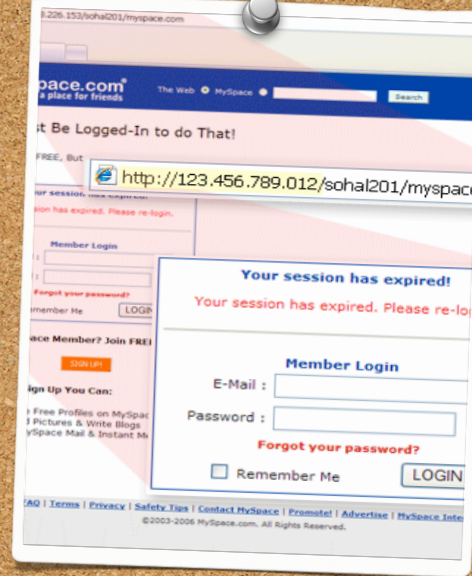
Infected computers become part of a controlled "army" of infected machines.

They can be used to send SPAM, viruses, or to initiate a DDoS (Distributed Denial of Service) attack on a website or network that can cause the website or network to stop responding altogether.

Phishing

Phishing attacks attempt to trick users into entering their login/credit card/SS#/etc into a fake version of a legitimate site so the sensitive data can be saved and used later by the attacker.

Many phishing attacks originate from e-mails and can be VERY convincing.



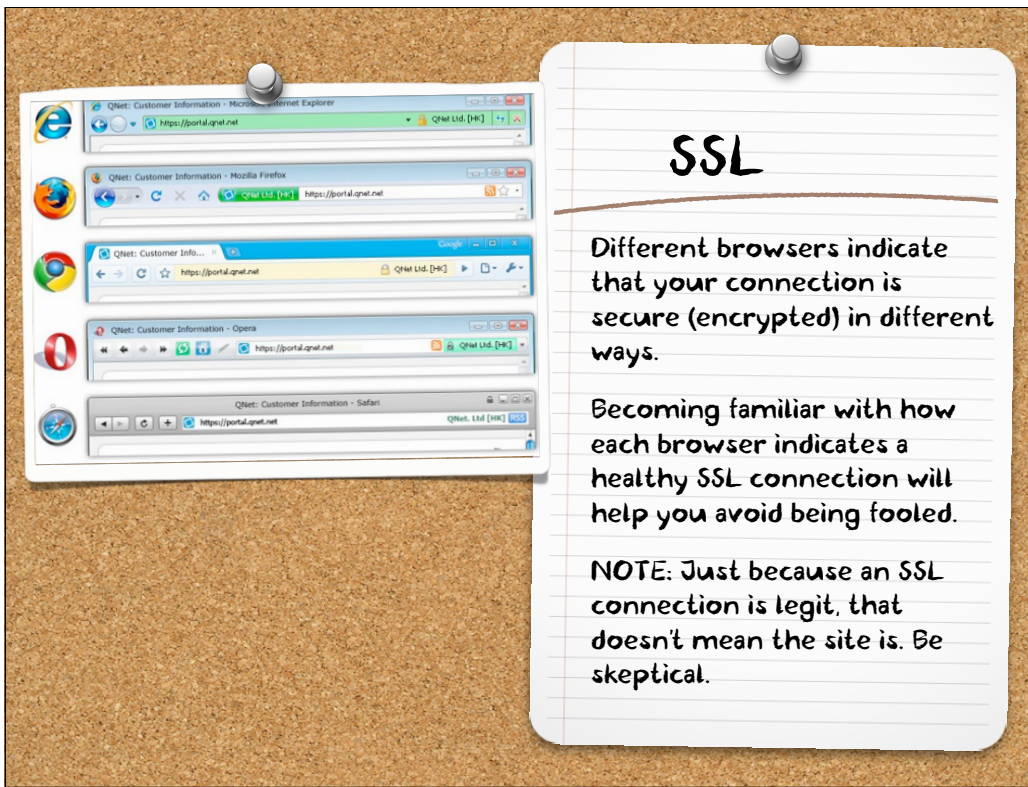
Phishers capture login information even for non-financial sites because they know that

MANY PEOPLE RE-USE THE SAME LOGINS FOR MULTIPLE WEBSITES.

[illegible]

Since Phishing scams take advantage of vulnerabilities in the human condition instead of vulnerabilities in technology, ALL users are at risk, whether they are on Mac, PC, Linux, etc.

[illegible]



SSL

Different browsers indicate that your connection is secure (encrypted) in different ways.

Becoming familiar with how each browser indicates a healthy SSL connection will help you avoid being fooled.

NOTE: Just because an SSL connection is legit, that doesn't mean the site is. Be skeptical.

Phishing & Smartphones

Smartphone users are particularly vulnerable to phishing attacks because the browser takes up the whole screen, and doesn't provide as much information about a page as a desktop browser.

This makes it easier to trick users into thinking the site is real.

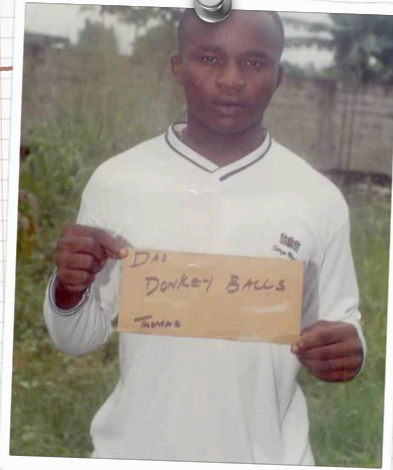


Case Study: Stanley Mark Rifkin

- In 1978, a computer tech stole \$10.2 million dollars from Security Pacific Bank using only social engineering.
- Talked his way into room where daily wire transfer security code was posted and memorized it.
- Called the bank, impersonating an authorized employee and requested a transfer of \$10.2 million to his swiss bank account.
- Because he was able to talk his way into learning the daily code, the transfer went through without a hitch. The woman who performed the transfer thanked him before hanging up.

"Social Engineering"?

- The act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques.
- Trickery or deception for the purpose of information gathering, fraud, or computer system access.
- In most cases the attacker never comes face-to-face with the victim.
- Social Engineering attacks are commonly executed over the phone or through email.



419 Scams

Nigerian Bank Scams (also called 419 scams after the section of Nigerian law it violates) are a type of advance-fee scam.

See:

419eater.com

scambaiter.com

"Message number 419" by MC Frontalot

Things to Watch For

- "Hi, I'm having a problem using the XYZ website. It's not working in my browser. I'm using IE7, what browser are you using?" Attacker can then target the attack based on vulnerabilities in the browser.
- "I'm having a problem using the website. Let me send you a link to the page I'm having trouble with." Link contains malware/phishing payload.
- "This is John Smith from XYZ Software Vendor. There was a critical security patch released that we need you to install or you are at risk of massive data loss."

Good Habits

- Shred ALL paper documents that contain intellectual property, financial or account information. Every time.
- If someone you do not recognize claims to be a new superintendent or maintenance worker, call downstairs to confirm before letting them in.
- If someone calls or walks in claiming to be a representative or worker from a company but you do not know them personally, call the company to confirm their identity and meeting.

PAY ATTENTION

- An attacker targets users of a website `myfantasyfootballleague.com` by finding people who post on the forums.
- The attacker sends them an email claiming a new feature or compromised account, directing them to `myfantasyfootballeague.com`, which they own. Note the missing third "l".
- Victim clicks and is phished, hijacked or tricked into downloading malware.

Case Study: Video Rental Shop

- Attacker Tom calls Jennifer at XYZ Video, claiming to be the manager of a different branch, asking if they have a copy of a video they can't find.
- Tom does this repeatedly over several weeks, building up a rapport with Jennifer and establishing the pretext.
- Tom then calls saying he has a customer of Jennifer's shop that forgot his membership and credit card but would like to rent from Tom's store. Jennifer provides that information to Tom to be helpful.

Attackers Will Research Their Targets

- After looking up the domain name records of a website, an attacker knows that someone named James Li is the technical contact. Tom calls James.
- "Hi, this is Bob Dickins from LuckyRegister. We have detected fraudulent activity on your account and we need you to reset your password."
- Vacation messages in email and voicemail can alert an attacker that you are out of town, giving them information that may help them sound legitimate to other people in the company

USB Keys

A very easy and often successful attack is to leave a poisoned USB key out where people can find it.

Who doesn't want a free USB drive?

The poisoned USB key infects the computer or entire network once it's plugged in.



Social Media

- Make sure your profiles are locked down so only friends can see your information
- Turn OFF geotagging on images in your Smartphone.

I Can Stalk U
Raising awareness about inadvertent information sharing

Home How Why About Us Contact Us

Who have we stalked recently?

- ICanStalkU was able to stalk [lead_myc](#) at <http://maps.google.com/?q=19.5668333333,-99.2036666667>
see them a minute ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to lead_myc](#)
- ICanStalkU was able to stalk [Alpha_Terran](#) at <http://maps.google.com/?q=51.3811666667,-0.333>
see them a minute ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to Alpha_Terran](#)
- ICanStalkU was able to stalk [Porchlomatica](#) at <http://maps.google.com/?q=29.4676666667,-98.559>
see them a minute ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to Porchlomatica](#)
- ICanStalkU was able to stalk [gruenter](#) at <http://maps.google.com/?q=50.4925,12.1423333333>
1 minute ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to gruenter](#)
- ICanStalkU was able to stalk [lserling](#) at <http://maps.google.com/?q=13.6310333333,-89.8452833333>
2 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to lserling](#)
- ICanStalkU was able to stalk [ellieeditor](#) at <http://maps.google.com/?q=52.3636666667,4.88>
3 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to ellieeditor](#)
- ICanStalkU was able to stalk [Bligferm0x](#) at 1710 Watson Ave New York NY
4 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to Bligferm0x](#)
- ICanStalkU was able to stalk [morgemoney](#) at I-65 Calera AL
4 minutes ago • [Map Location](#) • [View Tweet](#) • [View Picture](#) • [React to morgemoney](#)

Links

- Mayhemc Labs
- PaulDietCom
- SANS ISC
- Electronic Frontier Foundation
- Center for Democracy & Technology

[How did you find me?](#)

Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.
[read more](#)

[Help me fix this!](#)

Disabling Geo-Tagging on your phone is easy. Check our list of common phones.
[read more](#)

 **PLEASE ROB ME** 

Listing all those empty homes out there

Also follow our Twitter feed @pleaseerobme

Filter

Location

Twitter username

[Show everything](#) [Go](#)

Recent Empty Homes

 @wgrande left home and checked in less than a minute ago:
Aplicativo para iPhone adiciona fotos e videos aos check-ins do Foursquare. >>> <http://bit.ly/dm103> | #44q

 @TennesseeTwee left home and checked in less than a minute ago:
Feeding my addison @ Barbuckly <http://4sq.com/72b8v>

 @crinnygraham left home and checked in less than a minute ago:
I'm at Ten Horton w/ @tyrannemccarthy. <http://4sq.com/6CMV1v>

 @scanna283 left home and checked in less than a minute ago:
I'm at kindercare (1350 Wayne Way, San Mateo). <http://4sq.com/6w67b>

 @BMorePRGuy left home and checked in less than a minute ago:
I'm at Detroit Regional Chamber (One Woodward Ave, Jefferson Ave, Detroit). <http://4sq.com/6H0U88>

 @KingRican left home and checked in less than a minute ago:
I'm at Home. <http://4sq.com/6UJd7p>

More Info

Home
Why
About

Made Possible By

Foursquare
Twitter
@doyouwantit
@michiganmiami
@4sq

Join a Group

Find Coolest
Nearby Places
Search by State,
Feature,
Bedrooms. Get a
Great Custom
Home Plan Now!
www.4sq.com

Search, Burgle
Home
Search multiple
engines for search
burglows homes
www.4sq.com

Yeastle, Delightful
Try Yeastle!
Yeastle Delights
Just 100 Calories
Per Serving!
www.4sq.com

Bark, Robbery
Criminals
Find Free Legal
Information On
Bark Robberies -
Search

Location Services

Be careful using location services such as Foursquare, Facebook Places, etc if your social media accounts are open to anyone.

Gawker

Passwords

2516: 123456

2188: password

1205: 12345678

696: qwerty

498: abc123

459: 12345

441: monkey

413: 111111

385: consumer

376: letmein

351: 1234

318: dragon

307: trustno1

303: baseball

302: gizmodo

300: whatever

297: superman

276: 1234567

266: sunshine

266: iloveyou

262: fuckyou

256: starwars

255: shadow

241: princess

234: cheese

ALL Passwords Are Crackable

- Using an eight-core Xeon-powered system, Duo Security brute-forced 400,000 password hashes of the 1.3 million stolen from Gawker, cracking the first 200,000 in under an hour.
- 15 of the accounts for which it had cracked password encryption belonged to people working at NASA, nine were assigned to users employed by Congress, and six belonged to employees of the Department of Homeland Security.
- 2009 RockYou hack: "123456" was the most common password in the collection posted on the Web by hackers, followed by "12345," "123456789," "password" and "iloveyou"

There is NO Excuse for Shitty Passwords Anymore

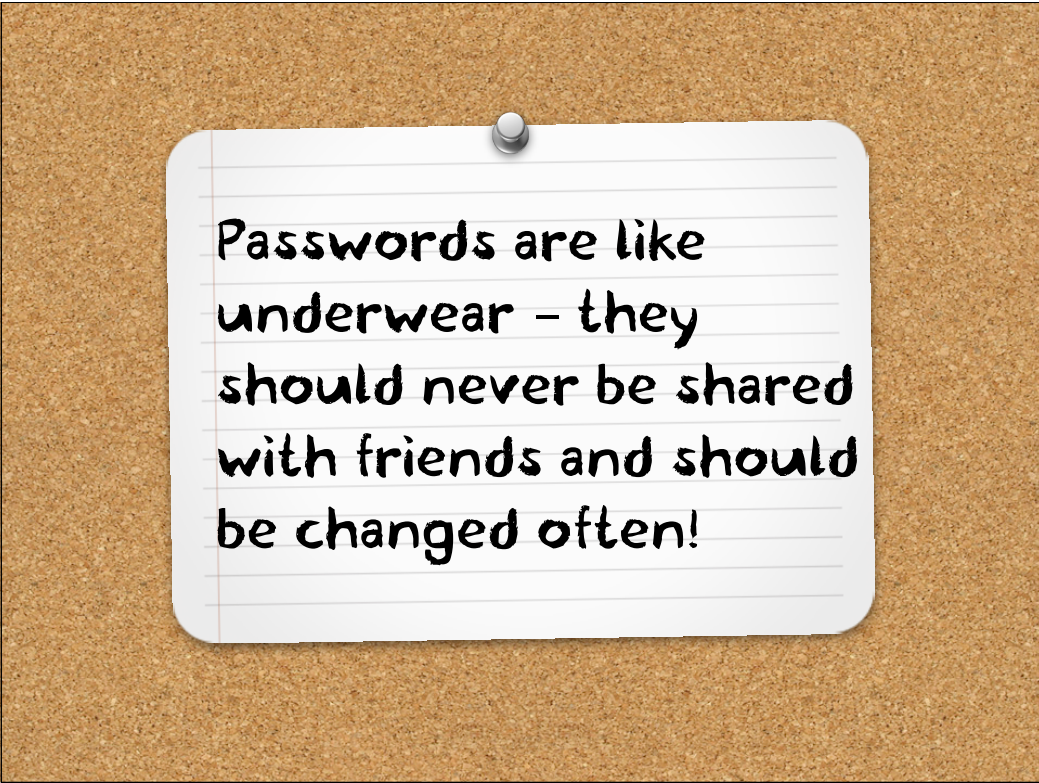
- 1Password and LastPass both allow you to:
 - generate long, highly random passwords that are unique to each website you log into
 - store the passwords in a database and auto-fill
 - sync that database across your iphone, ipad, other computers, etc.

Password Tips

- Don't use only letters or only numbers.
- Don't use names of spouses, children, girlfriends/boyfriends or pets
- Don't use phone numbers, Social Security numbers or birthdates.
- Don't use the same word as your log-in, or any variation of it.
- Don't use any word that can be found in the dictionary - even foreign words.
- Don't use passwords with double letters or numbers.

Password Tips

- Use the first letters of the words in a favorite line of poetry or a verse of song. "Hail, hail the lucky ones, I refer to those in love" becomes "H,hTL0,lR2t1L."
- EVERY SINGLE WEBSITE you have an account with should use a different password. You have no idea how secure their websites are, so you should assume they are not secure at all.

A corkboard with a light brown, textured surface. A white, rectangular note with rounded corners is pinned to the center of the board with a single silver pushpin at the top edge. The note has horizontal lines and contains text written in a black, handwritten-style font.

Passwords are like
underwear - they
should never be shared
with friends and should
be changed often!

Alison L. Gianotto

snipe@snipe.net

<http://www.snipe.net>

<http://www.un-hacker.com>

