



Internet Privacy and Security

Matthew Saltzman and Kathy Riley
LWVCA September 19, 2017



Topics

- Maintaining your own security
 - Passwords
- Maintaining your privacy
 - How your browsing history is tracked
 - What if a hack reveals your private information?
- Political issues related to the internet
 - Net neutrality
 - Privacy issues



Security

- Identity theft: Can somebody pretend to be you in some role?
 - Access to your accounts
 - Spoof your email, social media
 - Spend your money
 - Access private information
 - Lock you out



Social Engineering and Phishing

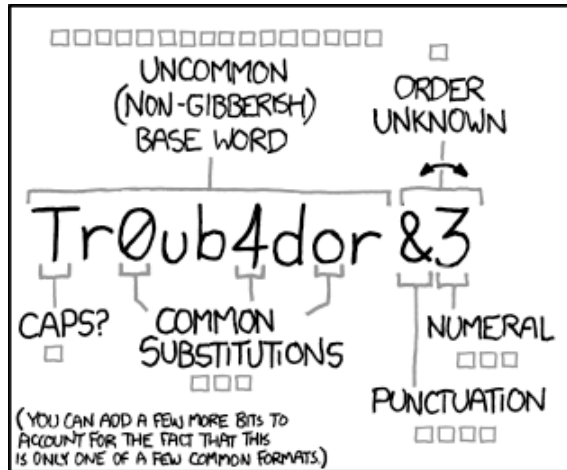
- “Social engineering” means convincing a victim to divulge personal information
- “Phishing” is an electronic form of social engineering
 - Send an email or otherwise convince you to click a link
 - Link downloads malware or leads to a spoof site asking you to log in or verify information such as account numbers
- “Spear Phishing” targets you directly



Passwords

- New guidelines for choosing passwords
 - Length is more important than alphabet or obscurity
 - Don't use personal information
 - Don't use the same password at multiple sites (especially sensitive ones)

Password Strength



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

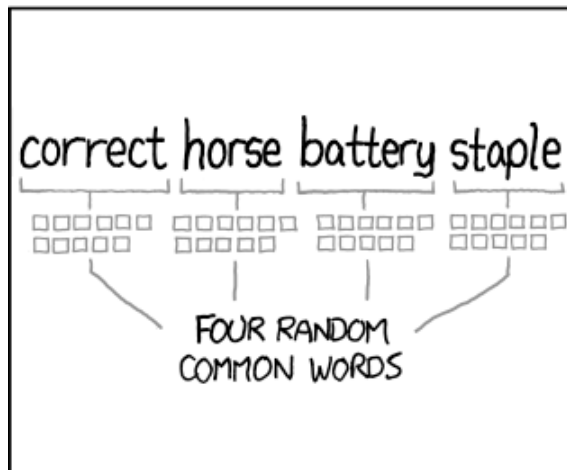
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Password Wallet

- Remembers passwords
- Generates strong random passwords
- Fills out Web and some app forms automatically
- You need only a master password
- Can be stored encrypted in the Cloud, accessible from multiple devices
- Firefox Sync, Lastpass, Keepassx, others



Two-Factor Authentication

- Password plus info only you can provide
 - Authenticator phone app
 - Generates random code or sends confirmation
 - Text message
 - Random code sent to you by SMS
 - Other communication with a device only you have access to
 - Biometrics
 - Fingerprint, retina scan, facial recognition



Securing Your Own Computer

- Check for and install security updates promptly
- Run a virus/malware scanner (not just Microsoft's!)
- Be careful what you share and how



Privacy

- Who tracks your browsing?
 - Sites you visit
 - (New!) Your ISP
- What if your data is stolen?



Tracking At Sites You Visit

- Good: A better browsing experience
- Bad: Sites collect and share personal data
- “Do not track” browser settings are widely ignored
 - You need to block sites that track
 - Note that this can break pages
- NoScript add-on for Firefox
- AdBlock+
- Privacy Badger (EFF)



Tracking By Your ISP

- You can't prevent your ISP from knowing where you go first
- HTTPS Everywhere (EFF)
 - Once at a secure site, interactions are encrypted
- Commercial VPN service
 - First stop is always your VPN
 - Read your VPN terms of service!
- The Onion Router and TOR Browser
 - Adds indirection and encryption



Your Privacy and Your ISP

- In April, Congress blocked strong Obama FCC rules on internet privacy
 - ISPs could, in principle, sell your browsing history
 - Not likely they will do so directly



Equifax!

- Attack vector likely through uninstalled security patch and insecure password(!)
- What you can do
 - Create Social Security Online account
 - Freeze credit reports
 - Enable fraud alerts
 - Monitor your accounts
 - Watch out for tax return fraud



Net Neutrality

- In a neutral net, your ISP can't advantage or disadvantage content providers based on who they are
- Without neutrality, your ISP could block or slow competitive sites or prioritize paying clients or their own content
- Currently, ISPs are subject to "common carrier" rules, but those rules may be weakened by current FCC



Other Current Issues

- Stop Enabling Sex Traffickers Act (SESTA)
 - Makes social network providers responsible for content of posts by users
- Warrantless searches of devices at border stops
- Etc.
- Advocacy
 - Electronic Frontier Foundation (<https://www.eff.org>)