#edsec: A Crash Course in Privacy + Security for the Classroom

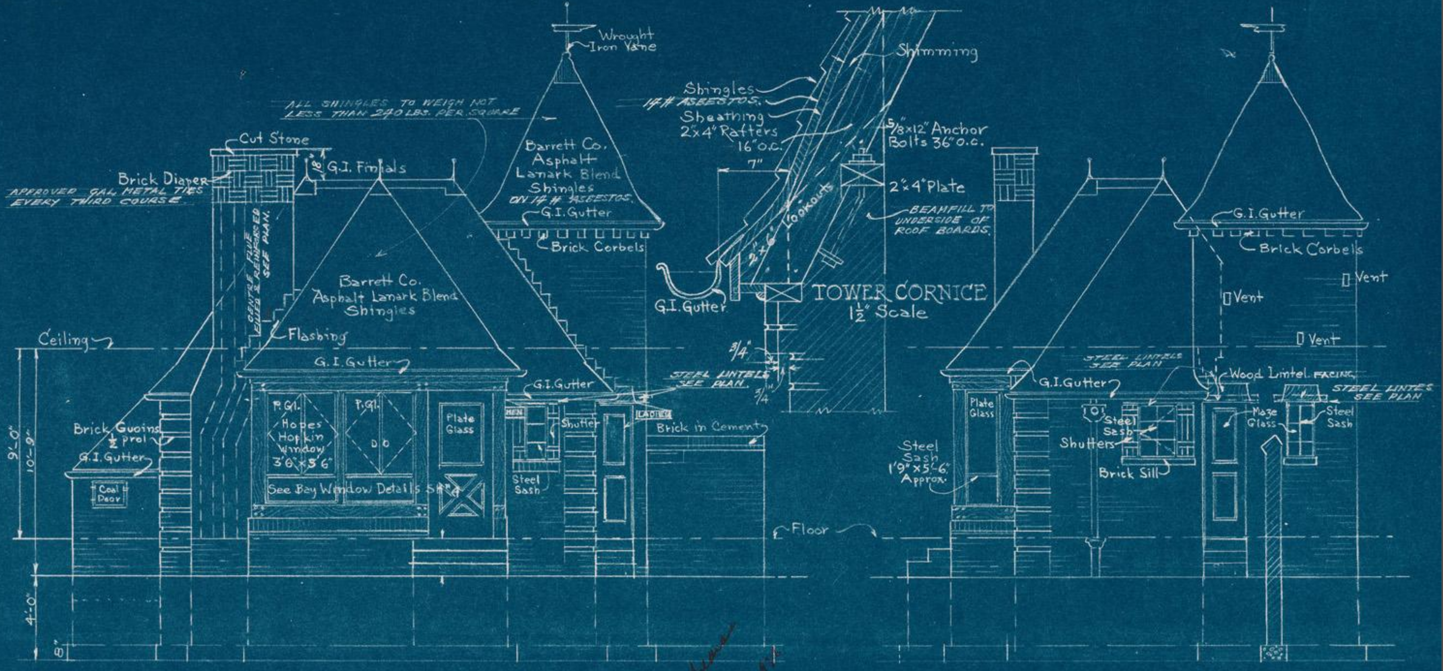
SVCUE 2016

Jessy Irwin

@jessysaurusrex

NB: Be sure to view the speakers' notes!

Who am I?



TOWER CORNICE
1½" Scale

FRONT ELEVATION
¼" Scale

RIGHT SIDE ELEVATION
¼" Scale

Approved re appearance
Nov 17 19[illegible]

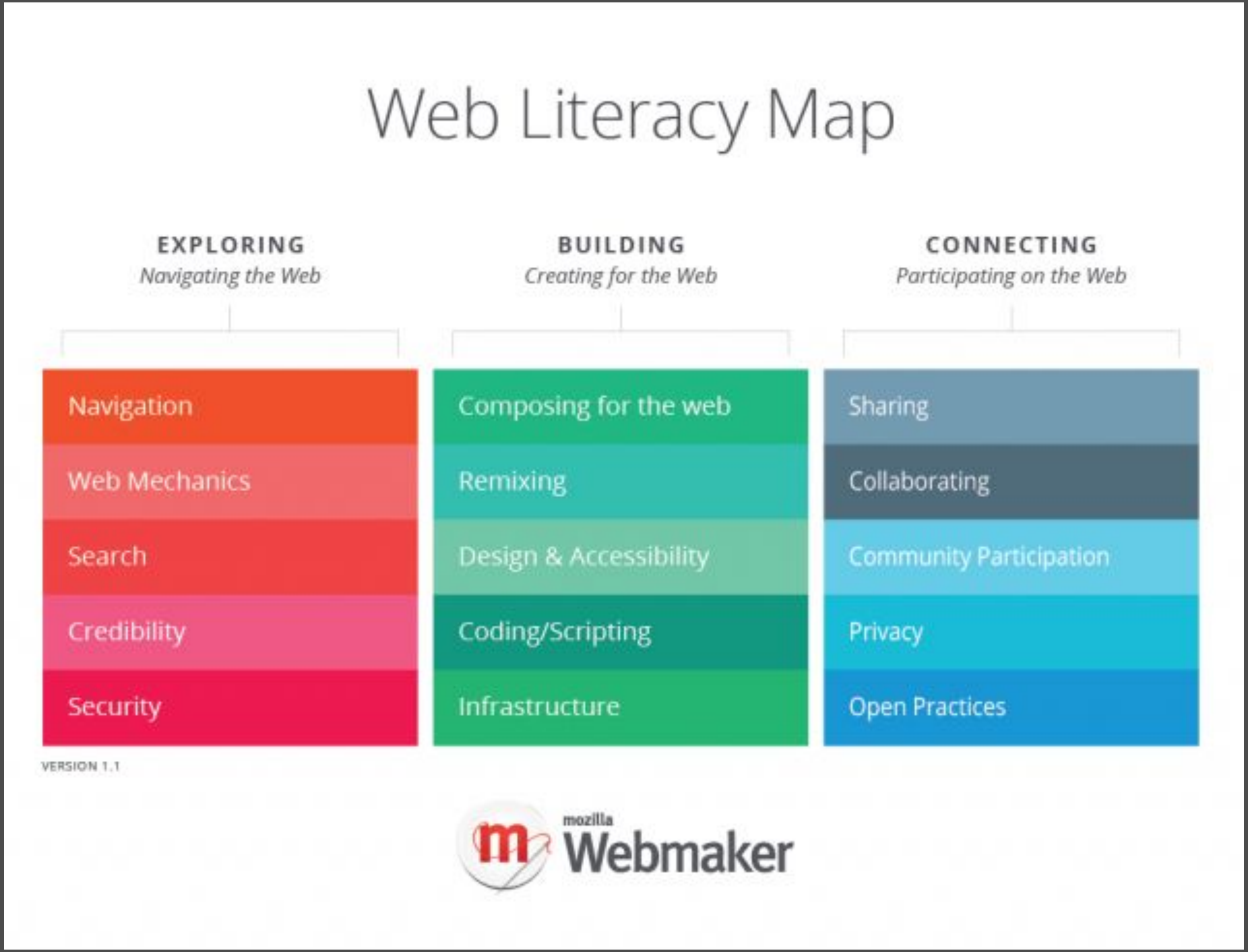
ACB

G.I. = Galvanized Iron

ONTARIO
Revised Aug. 20, 1936

JOB # 834	SHEET # 2

CVE-2014-0160



Web Literacy Map

EXPLORING *Navigating the Web*	BUILDING *Creating for the Web*	CONNECTING *Participating on the Web*
Navigation	Composing for the web	Sharing
Web Mechanics	Remixing	Collaborating
Search	Design & Accessibility	Community Participation
Credibility	Coding/Scripting	Privacy
Security	Infrastructure	Open Practices

VERSION 1.1

mozilla Webmaker

Warning: these are not actual hackers :)

Warning: these are not actual hackers :)

Operational Security

Separate your personal and professional accounts!!!

Use certain apps for specific purposes-- i.e. communication.

Physical security

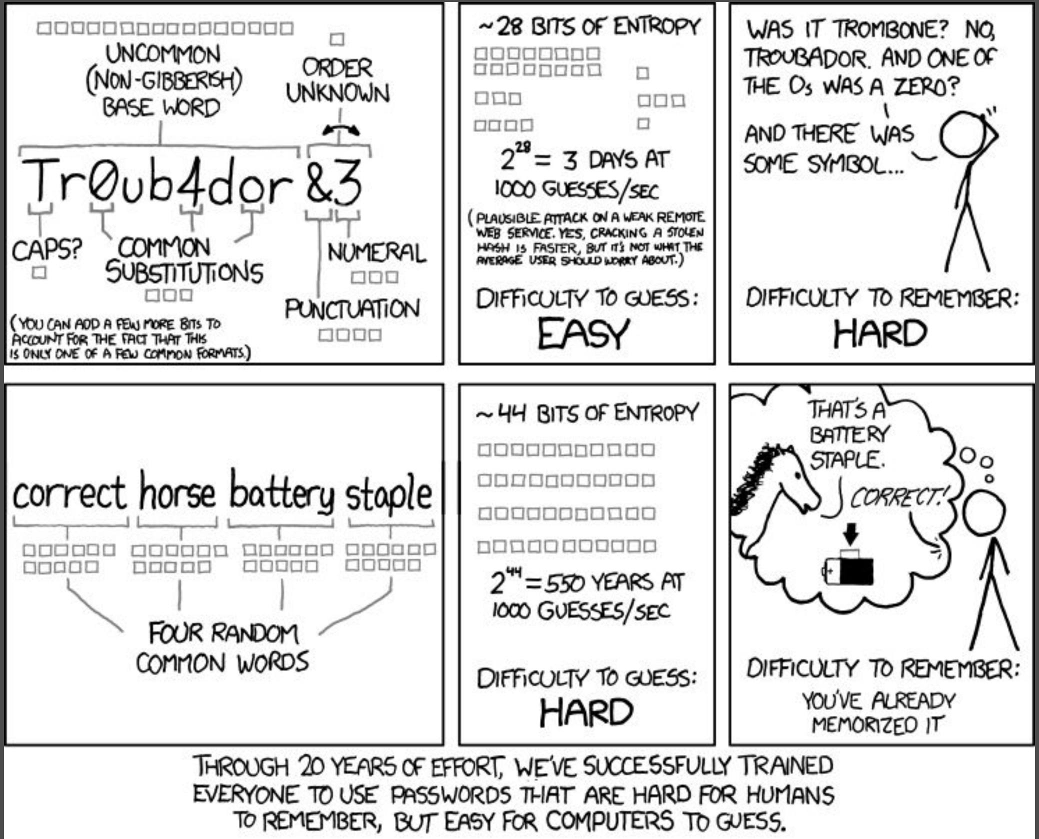
- Set up strong passcodes on mobile devices, screensavers on desktops + laptops
- Create screenlocking shortcuts in Settings/Preferences for displays when you're away from your device.
- Back up your data! Data loss = awful.

Protect your secrets

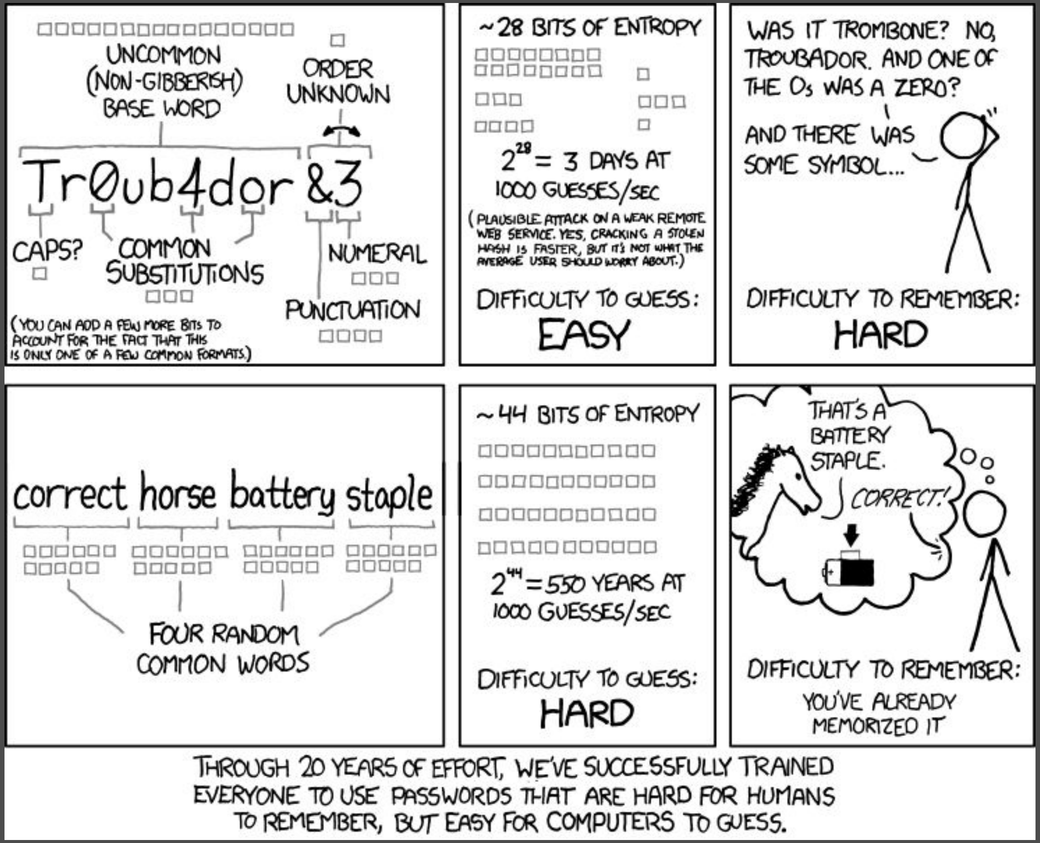
Google hacking

- search with filename: .xls/.doc operators

Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

Passwords

- NO SPREADSHEETS!!!!1!!1! EVER!
- Use a password manager: **1Password** (or LastPass, Dashlane, KeePass, etc.)
- haveibeenpwned.com is great for breach notification

2-factor authentication

Google Authenticator
~* or *~ your password manager

~* This is a must for social media and personal email accounts! *~

Avoid common online attacks

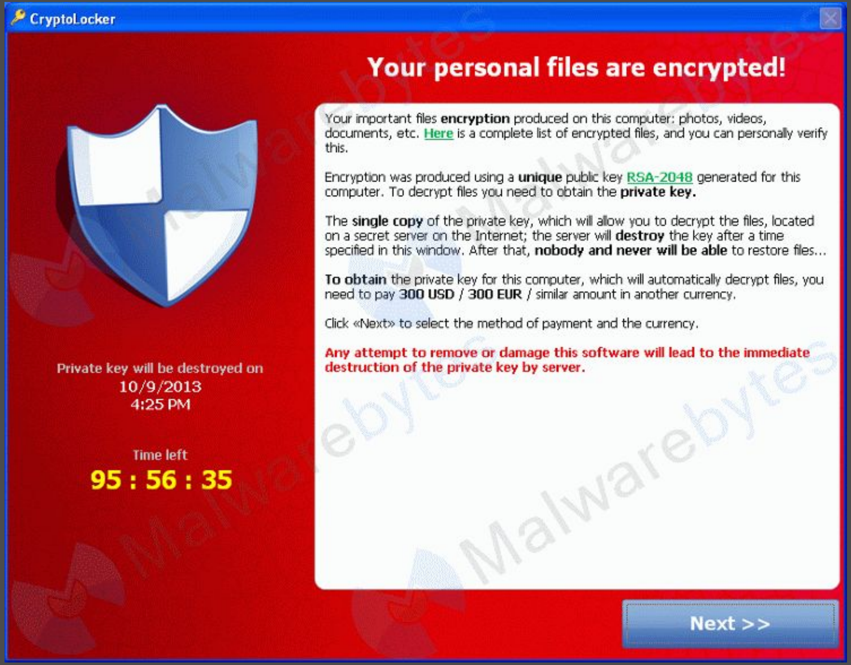
[Phishing]

[Malware]

Ransomware

Spoofing

Spyware



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Other security tips

- Update browsers + software regularly
- Use an adblocker like uBlock
- OpenDNS
- HTTPs Everywhere

Beware of public wifi: use a VPN, or BYOI

Use sample data when testing a new service

How can we model online security to our students?

Security is what we use to give people (our students!) privacy. How can we evaluate whether a tool is secure enough to protect student privacy?

edtechinfosec.org

How can we evaluate whether a tool protects student privacy?

funnymonkey.com/blog

You've made it to the end! Here's a puppy.

Email me any time with questions: jessy.irwin@gmail.com