

Security (Continued)

Peter Nore

LastPass for anti-phishing or url-baiting

- LastPass is a password manager that integrates into browsers
- One strong password opens up all your other passwords
- Password bundle is encrypted with your password using JavaScript running on your machine and then synchronized with a server over HTTPS
- *By only clicking on a link to "gmail" in LastPass, you can make sure you are always going to the same address*
- This is important to make sure you don't type in "gnail.com" by accident

LastPass cont'd

Security Strengths:

- Tools to generate passwords are right in the browser
- Your info is encrypted in the browser with 256-bit AES and *before* it is sent over SSL - even if people hack LastPass, your data is safe if you have a good password

Security Vulnerabilities:

- If a bad guy knows you use last pass, it could up the danger of a keylogger.
- Then again, if you have a keylogger, chances are you don't have much hope anyway.

What's a keylogger?

- Records all keystrokes with a timestamp
- Can be physical or software-based
- It's fairly easy to write software to tell when passwords are being entered in retrospect



How do people get keyloggers?

- Assuming you are not targeted by the FBI, most people get keyloggers from drive-by downloads
- Good anti-phishing and anti-malware computer hygiene will protect you in most cases - but not guaranteed
- Use one-time passwords if suspected of keylogging
- Assume that internet cafe's have keyloggers - do not plug USB drives in and then infect your computer at home
- <-- Use two-factor authentication



Phishing Example

From: info@hbs.edu [mailto:dngprojects@telenet.be]

Sent: Monday, September 26, 2011 12:35 PM

Subject: "hbs.edu" IT HELP DESK.

This message is from hbs.edu Email Administrator to all our email account subscribers. Due to the recent attack on our database by a new virus called SPEK155. We are currently upgrading our database and all accounts need to be re-validated and upgraded to the new 2011 anti-spam version. You are advised to provide us the below information within the next 72 hours so that your account can be re-validated and upgraded to the new 2011 anti-spam version or you stand a risk of having your account De-activated from our database due to the menace of this virus.

User Name:

Password:

Confirm Your Password:

Thank You.

hbs.edu Administrator

Warning Code :ID67565434.

Social Attacks

Figure 25. Paths of social tactics by percent of breaches within Social

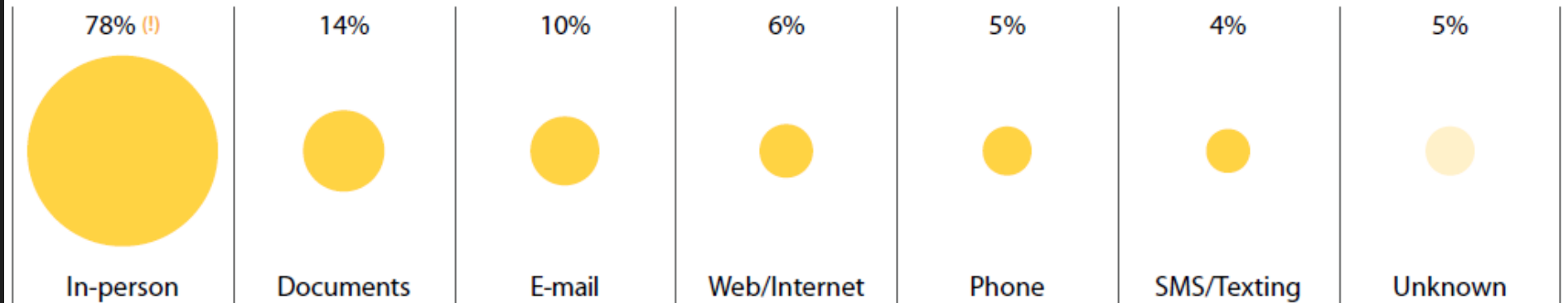
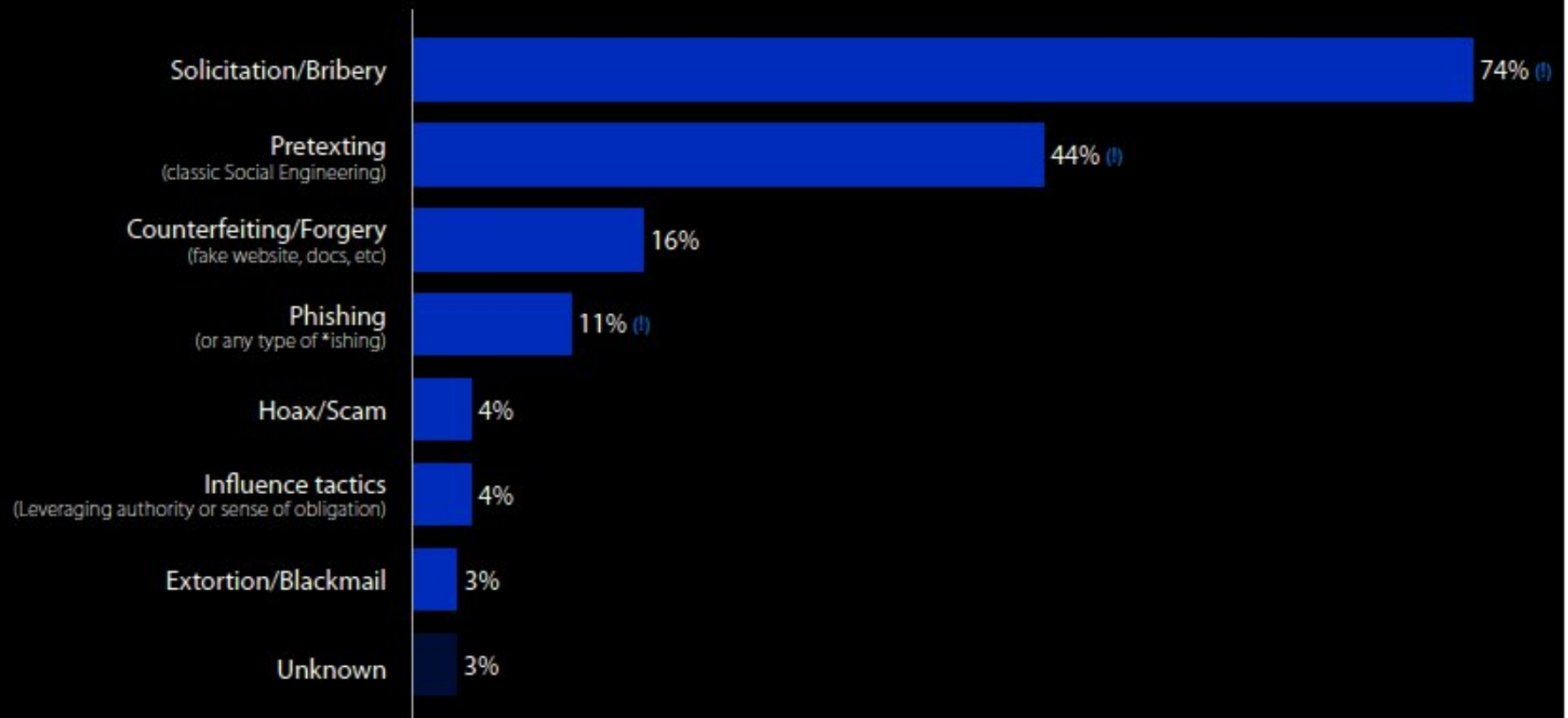
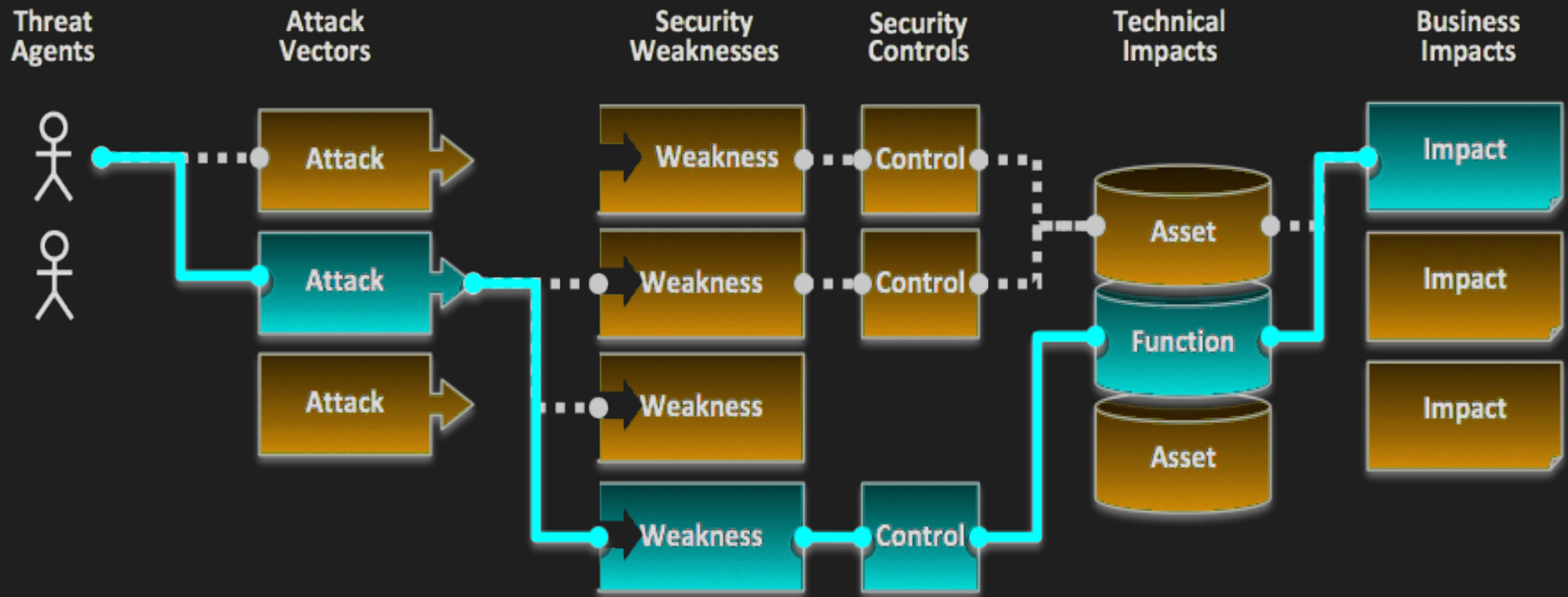


Figure 24. Types of social tactics by percent of breaches within Social



Attacks take advantage of vulnerabilities at every level



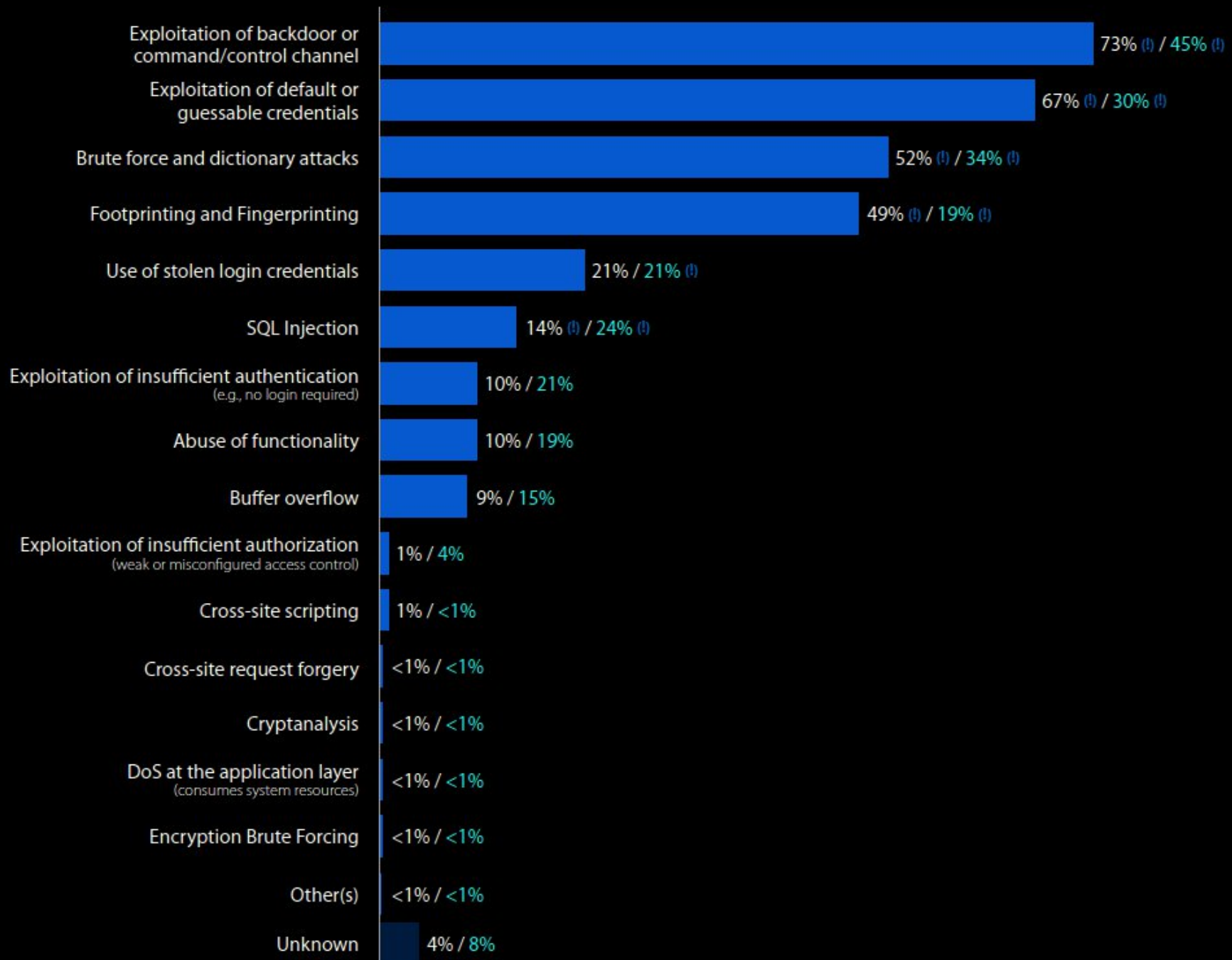
source: OWASP

Types of Hacking We Haven't Discussed

- Footprinting
 - Discovering what IP addresses are owned by the target
 - Gathering publicly available information about a potential target
- Fingerprinting
 - Using that publicly available info to profile a target and do more research
 - Systematic survey of all of the target organization's Internet addresses for certain functionality - port scanning, etc

Types of Hacking

Figure 22. Types of hacking by percent of breaches within Hacking and percent of records



TrueCrypt Demo

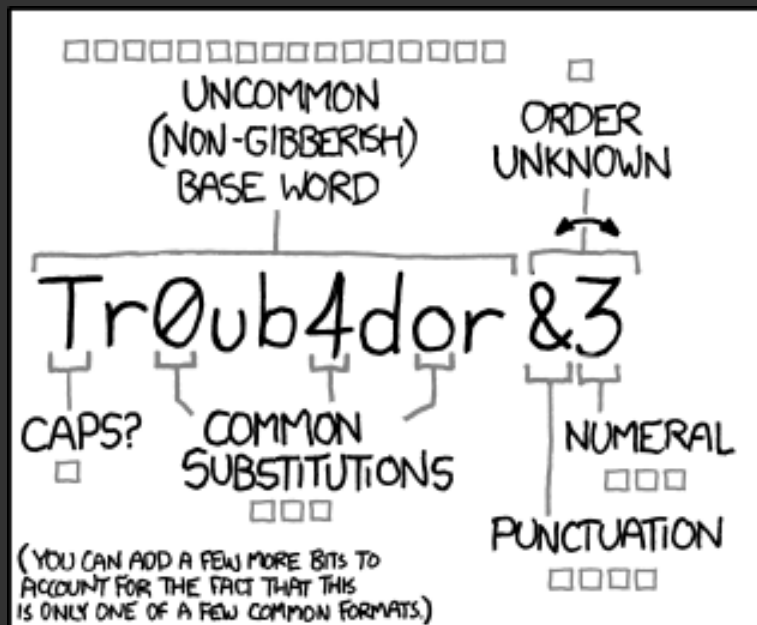
<http://www.truecrypt.org>

Why encrypt?

- Encryption is the only way you'll ever know information is safe when at rest
- You never know who will find your data after the fact
- Protect financial information
- Protect against identity theft
- You owe it to your friends and contacts
- If identity theft happens, you'll need to know better what did not cause it
- Don't let your computer be a site of reconnaissance for your employer
- Political dissent, workplace dissent, etc.
 - "locks are meant to keep honest people honest"

How to make a good password

- Pick a quote
 - "An apple a day will keep the doctor away"
- Memorize it
- Turn it partially into an acronym, but leave at least one word
 - AAADWKTDctorA
- Replace some letters with their "LEET" alphabet equivalent
- LEET:
 - 4aADWk7d0c70RA
- Now use it once a day and say the quote while you type it - soon, it will be automatic
- Learn a new password every six months



~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.)

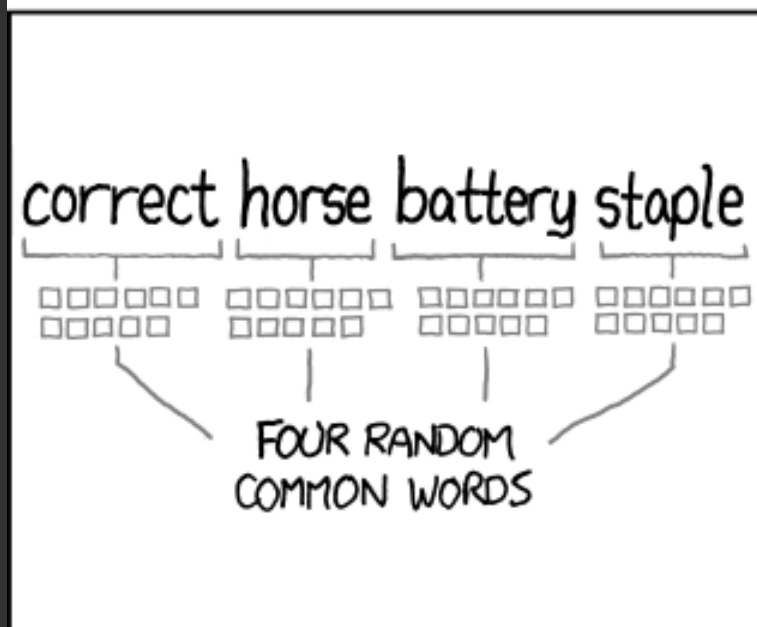
DIFFICULTY TO GUESS: **EASY**

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

AND THERE WAS SOME SYMBOL...



DIFFICULTY TO REMEMBER: **HARD**



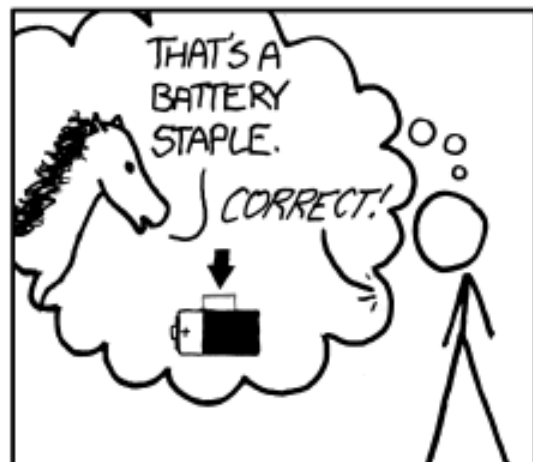
~44 BITS OF ENTROPY

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

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.

"Trust, Trust but Verify"

The more people that
aren't criminals that can
think like criminals,

the fewer opportunities
will exist for easy
exploitation.

Security is a web of trust.

Consider using a virtual machine for online banking. An easy one developed by David et al:

https://manual.cs50.net/CS50_Appliance

[2.3](#)