
TuffPass

Problem?

Who Hacked Yahoo? Who Cares!
Bloomberg - Sep 22, 2016
That line from Bloomberg News' coverage of the **Yahoo hack** of at least 500 million user accounts sums up the ridiculous attitude so many in ...

Yahoo Hack: Who Got Hit, Where, and How to Protect Yourself
Voice of America - Sep 23, 2016
The **hack** of 500 million **Yahoo** user accounts is far and away the largest corporate breach ever reported, ahead of the 2013 MySpace **hack** that ...

Recode's Kara Swisher Discusses **Yahoo**! (YHOO) Email **Hack** ...
TheStreet.com - Sep 22, 2016

View all

Even if you don't use Yahoo, you're probably still at risk from its hack
Quartz - Sep 26, 2016
Yahoo isn't exactly king of the hill in Silicon Valley anymore—it's more like over the hill by Valley standards. But the news that half a billion user ...

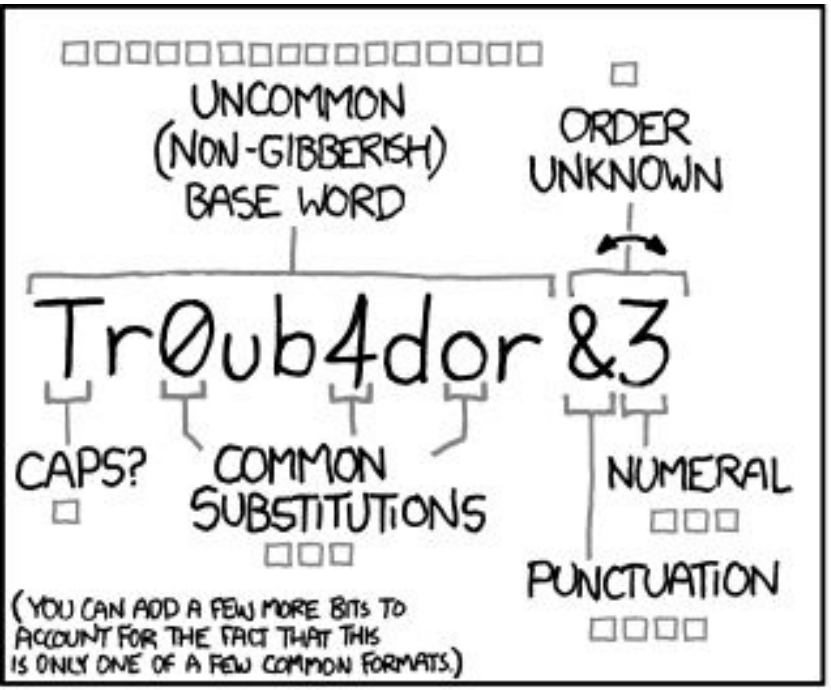
Report: Yahoo to Confirm This Week That 200 Million Accounts ...
New York Magazine - Sep 22, 2016
Recode reports that **Yahoo** is getting ready to confirm a widespread ... and the **hack** could be costly if government investigators and other legal ...

Security News This Week: Verizon Reportedly Wants a $1 Billion ...
WIRED - Oct 8, 2016
Remember that **Yahoo hack** that compromised half a billion email accounts? Verizon does, too. And according to the New York Post, Big Red ...

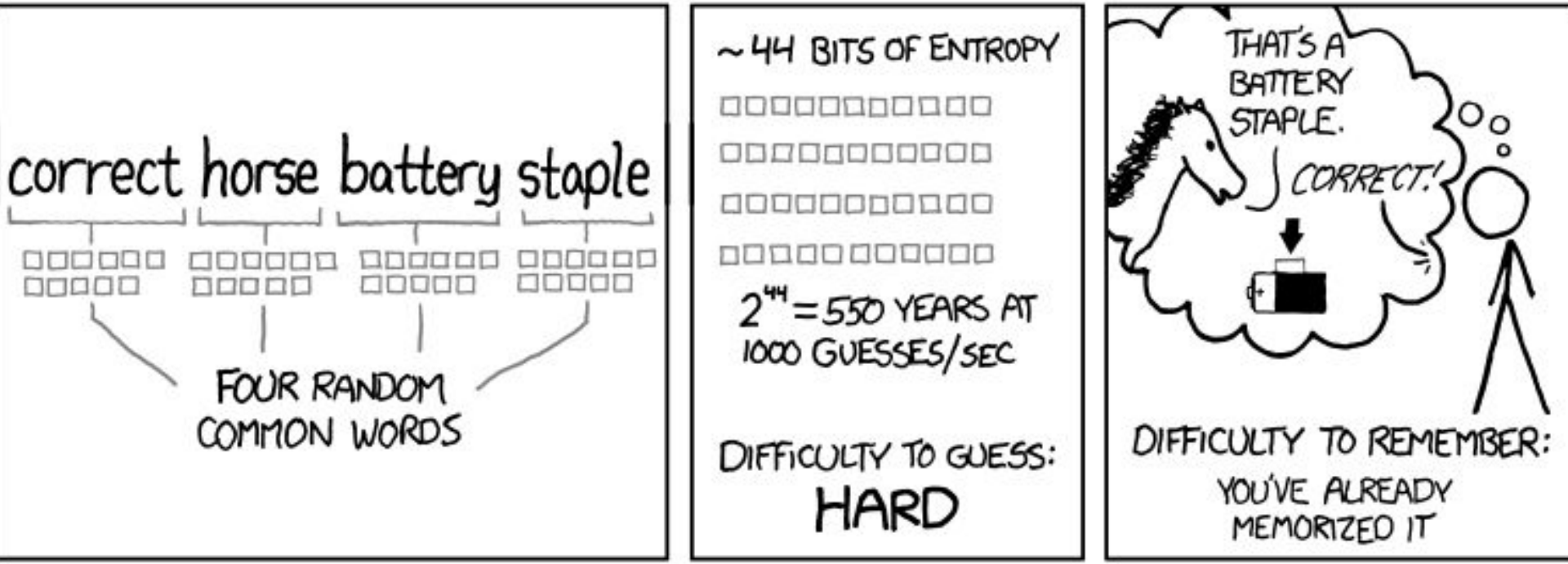
YHOO Stock: Is Verizon Reconsidering the **Yahoo** Deal?
Wall Street Pit - 7 hours ago

Easy, just use unique passwords!

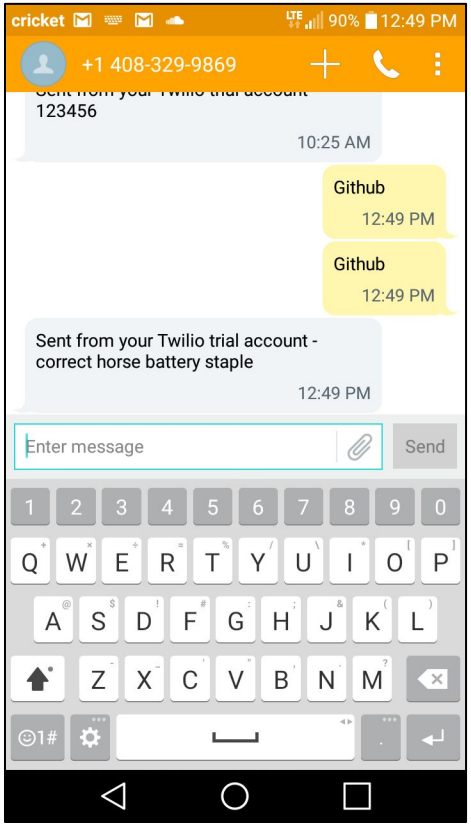
The traditional way



The XKCD way

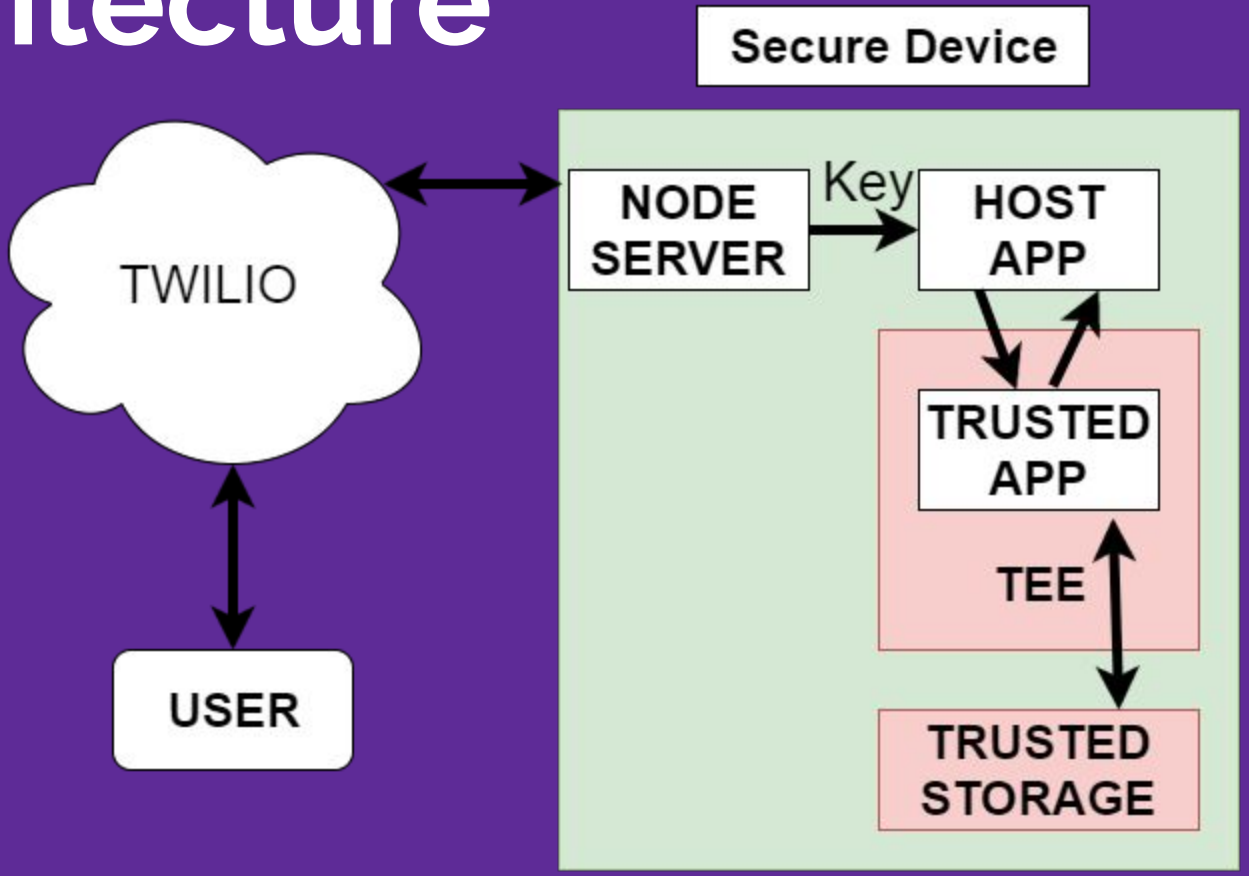

correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT

How it works



- Text service name
- Password generated, written to TEE storage
- Twilio replies w/ password, create/change your password for that service
- Text service name again at any time to retrieve the password

Architecture



How is this better?

- Passwords are generated in the TEE and encrypted in Trusted Storage
- No additional hardware/software
- Runs on hardware under ***your control***!

Future Work

- Android app rather than text interface with secure connection to server
- Open source the server for increased adoption and improved security auditing

TuffPass
Trusted Password Generator

Synopsis

TuffPass generates memorable passphrases entirely in the secure TEE area of supported devices and is encrypted at all times. Unlike other password managers, the data is not synced to third parties, and no additional software or hardware is required. The encrypted passphrases are retrieved by the user, any time and anywhere, by sending a text message from a verified phone. All the while, the TuffPass device is stored in a secure location, under the user’s complete control!