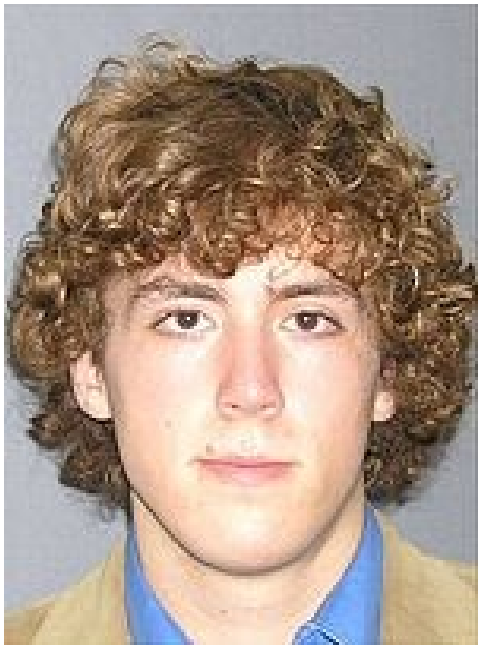
Security

It’s for everyone,
not just the paranoid.

Passwords



In 2008, David Kernel obtained access to Palin's account by looking up biographical details such as her high school and birthdate and using Yahoo!'s account recovery for forgotten passwords.

Kernell was sentenced on November 12, 2010, to one year, followed by three years of supervised release.

P4ssw0rd

These are all pretty much useless:

Kissme

Harvey

1L0vey0u

Daff0dil

B4byd0ll

“If you liked it then you shoulda put a ring on it”

=

1yl1tyspar01

It can be individualized:

=

1yl1tyspar01Instagram?

Phishing and “Spear Phishing”

Subject: *Someone has your password*

Hi John.

Someone just used your password to try to sign in to your Google Account:
john.podesta@gmail.com.

Details: Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt.
You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team

Charles Delava's reply (with typo, missing "not")

Sara,

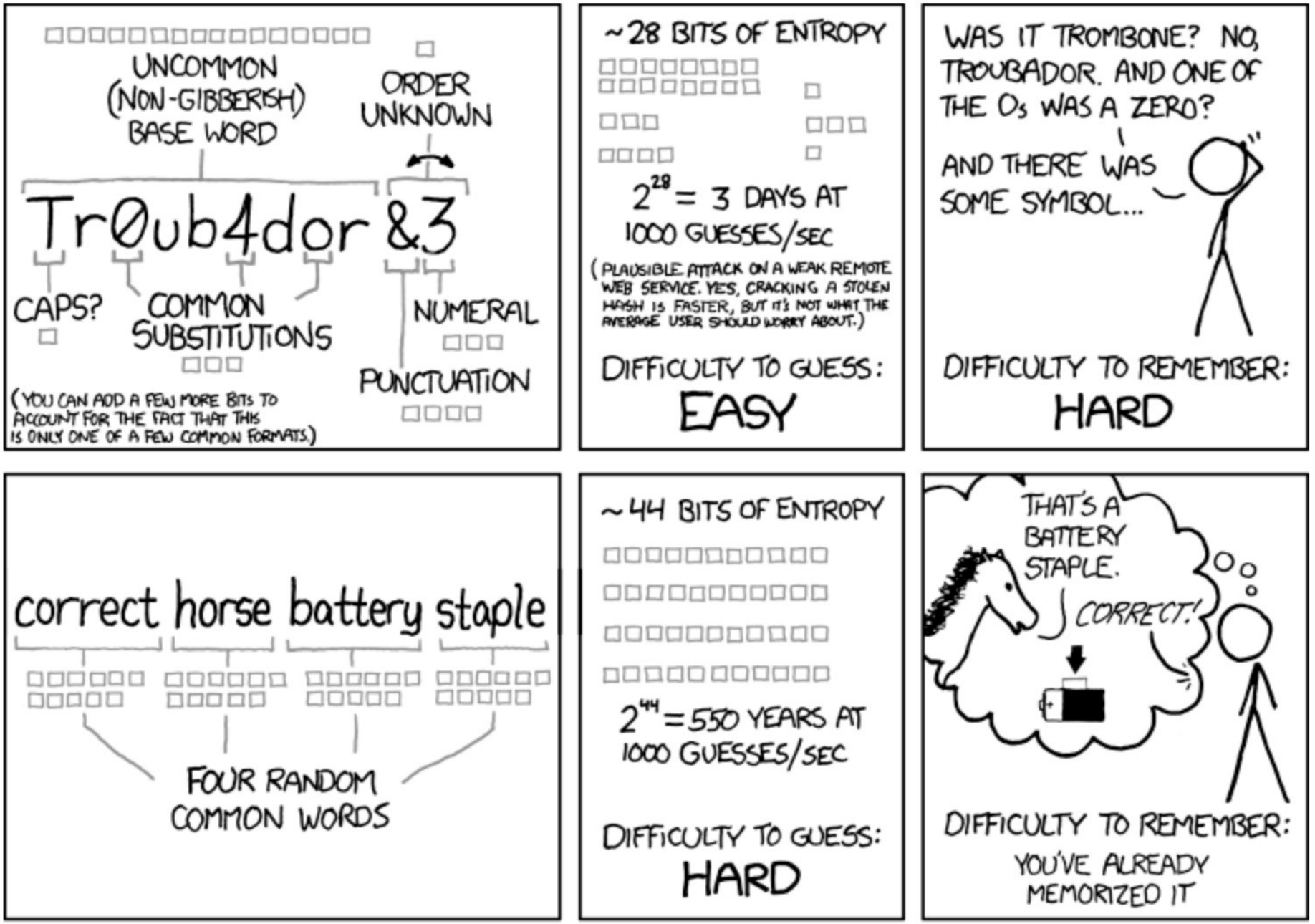
This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security

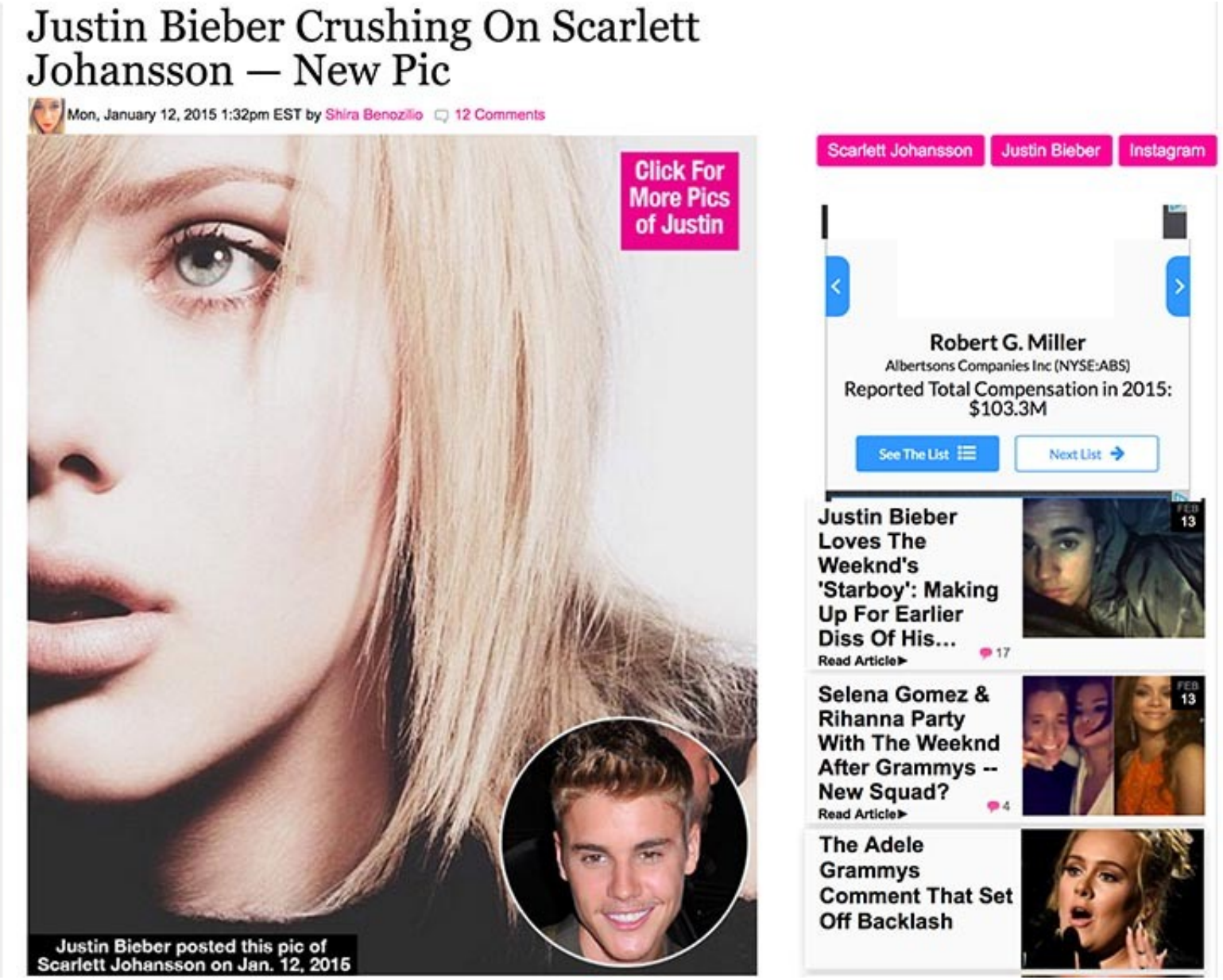
to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at [redacted]

(XKCD comic)


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.

Phishing and “Spear Phishing”



“Is This Something That’s Going to Haunt Me the Rest of My Life?”

IT professional, Charles Delavan
(-on Hillary Clinton’s hacked emails in the 2016 Presidential election.)

Clinton advisor John Podesta with Clinton during a press conference

spear phishing email to John Podesta:

Subject: *Someone has your password*

Hi John.

Someone just used your password to try to sign in to your Google Account:
john.podesta@gmail.com.

Details: Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt.
You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team

Charles Delavan's reply (with typo, missing "not")

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security

to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at [redacted]

Google

Account help for dmoser@massart.edu

Answer the following to verify this account is yours.

Enter the last password you remember

••••••••••••••

Next

Try a different question

dmoser@massart.edu
Use a different account

On Oct. 7 2016, the Department of Homeland Security and Office of the Director of National Intelligence on behalf of the **U.S. Intelligence Community issued a joint statement:**

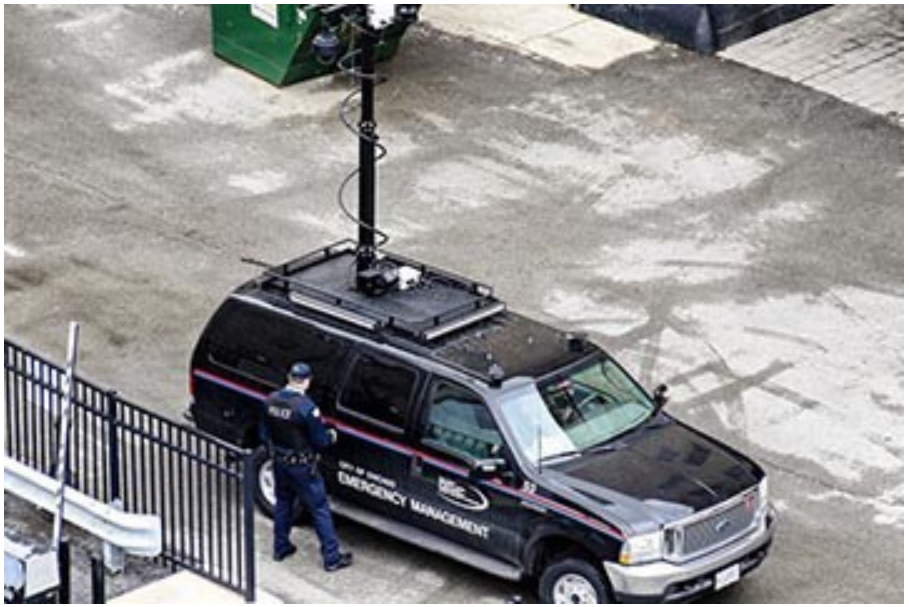
"The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations.

The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process.

We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities."

Technological innovators usually don't ask the courts before marketing products.

Harris Corp. product: “The StingRay”



Masquerades as a cell phone tower, then forwards numbers, reverse user-lookups, force phone power drain, etc.

- NSO Group, Israel
- The Hacking Team, Italy
- US Government

Malware Technologies for “National Security”

Companies create malware that exploit previously unknown and unpatched zero-day vulnerabilities in phone operating systems.

The malware can silently jailbreak an iPhone when a victim, through spear-phishing, is sent and opens a malicious URL.

After a user opens this link, the malware installs on the phone, hoovering up all communications and locations of the targeted iPhones including iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram and Skype communications and it can collect Wi-Fi passwords.

Ex: “Researchers noticed that the malware's code referenced an NSO Group product called 'Pegasus' in leaked marketing materials... It had previously been sold to the government of Panama..”

Ex: “StuxNet” worm to sabotage Iranian nuclear reactors.

China: “Sesame Credits”

"Zhima xinyong"
(http://zmxy.antgroup.com/index.htm)

"Gamification" of good citizenship

- Collaboration between gov't and largest game co's.

- Integrated with social media

- Friends with low scores drag your down

- High scores give perks in government paperwork