Digital Security in the Real World

https://bitly.com/jplus-security

Mike Tigas, ProPublica

Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption

Millions of documents show heads of state, criminals and celebrities using secret hideaways in tax havens

By The International Consortium of Investigative Journalists
Apr 3, 2016

A massive leak of documents exposes the offshore holdings of 12 current and former world leaders and reveals how associates of Russian President Vladimir Putin secretly shuffled as much as $2 billion through banks and shadow companies.

What's Really at Stake in the Apple Encryption Debate

The government has never been allowed to create a "backdoor" to encrypted devices. Now, it's trying to force Apple to build one.

by Julia Angwin
ProPublica, Feb. 24, 2016, 3:29 p.m.

46 Comments | Print

A protestor holds up an iPhone outside of the the Apple store on 5th Avenue on Feb. 23, 2016 in New York City. (Bryan Thomas/Getty Images)

The FBI's much-discussed request to Apple can seem innocuous: Help us extract six

US news

US government secretly obtained Associated Press phone records

Justice Department obtains two months of records in what AP's top executive calls 'massive and unprecedented intrusion'

Associated Press in Washington

Monday 13 May 2013 17.05 EDT

AP president and chief executive officer Gary Pruitt sent a letter of protest to Attorney General Eric Holder. Photograph: Jacquelyn Martin/AP

The US Justice Department secretly obtained two months of telephone records of reporters and editors for the Associated Press in what the news cooperative's top executive called a "massive and unprecedented intrusion" into how news organizations gather the news.

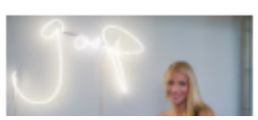
Most popular in US

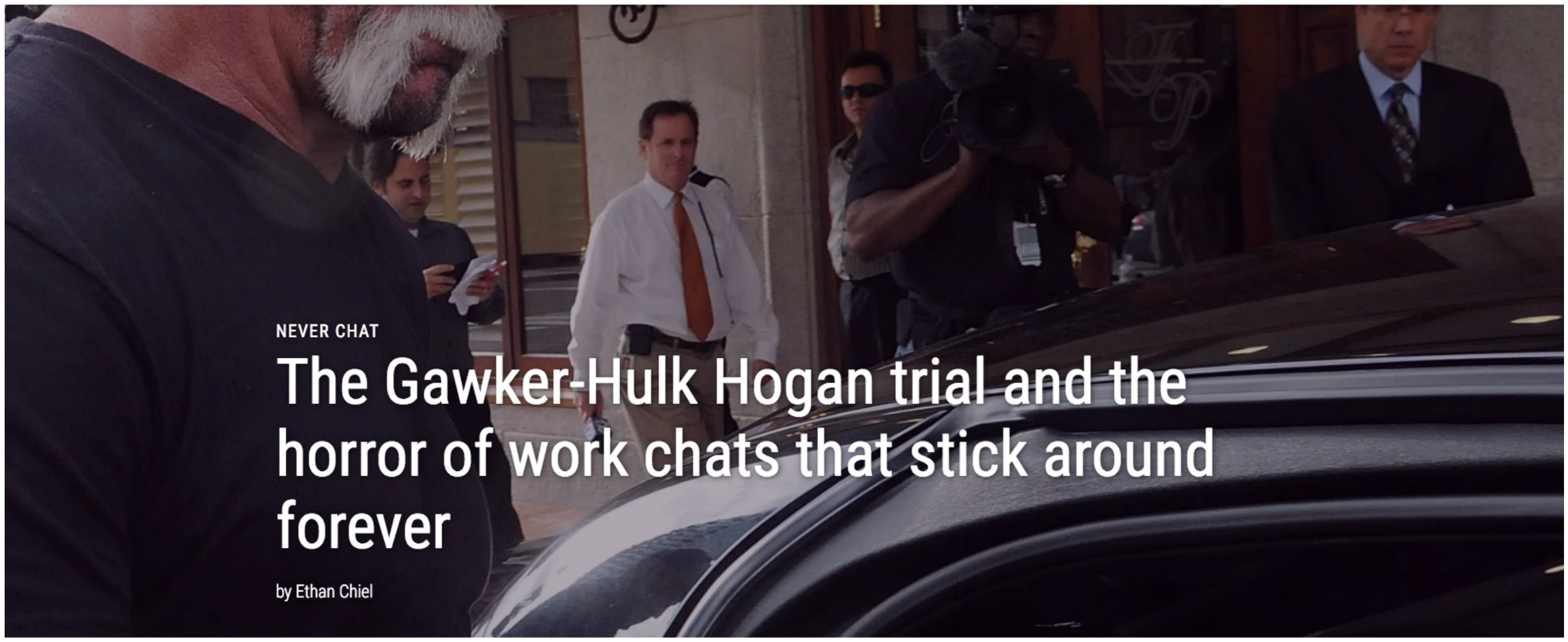

World's carbon dioxide concentration teetering on the point of no return


Queen caught on camera saying Chinese officials were 'very rude'


Tokyo Olympics: €1.3m payment to secret account raises questions over 2020 Games


Scores of people killed across Baghdad in three car bomb attacks


The joylessness of Goop sex | Flic Everett



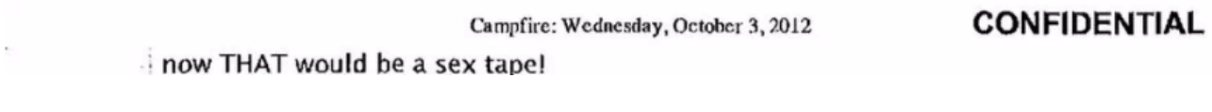
NEVER CHAT

The Gawker-Hulk Hogan trial and the horror of work chats that stick around forever

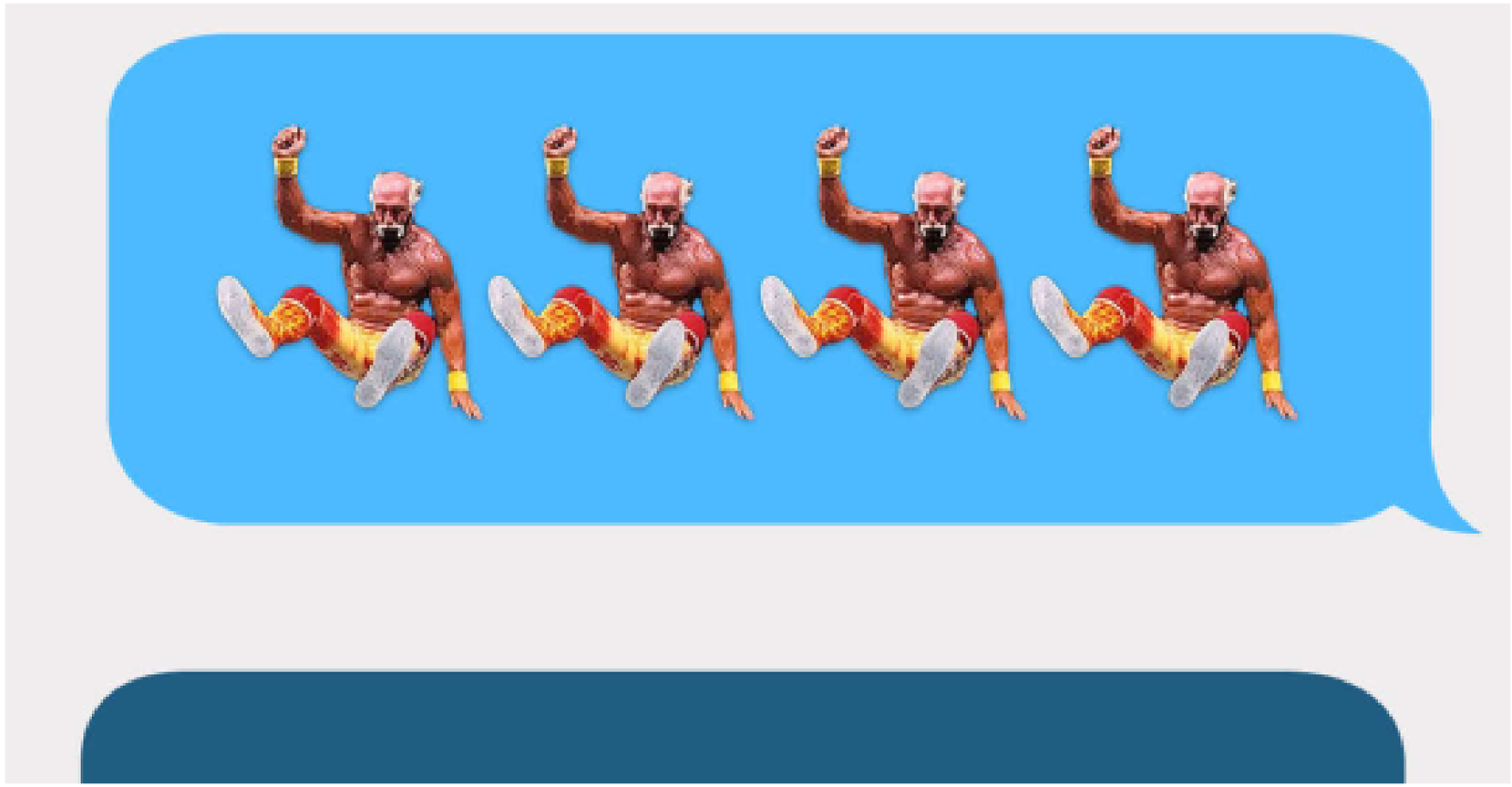
by Ethan Chiel

March 9, 2016 12:03 p.m.

This week, Hulk Hogan's multi-million dollar lawsuit against Gawker for posting his sex tape finally went to trial. The Florida jury trial, with its testimony on penis size and extramarital sex, is almost as NSFW as the video itself, an excerpt of which Gawker posted in 2012—and then took down after being sued. But what was really on our minds watching the proceedings via livestream is the reminder that every time you send an email to a coworker or type a message in an intra-office chat room you should imagine that someday your words will be read out loud in open court.


Campfire: Wednesday, October 3, 2012 CONFIDENTIAL

now THAT would be a sex tape!



I spent part of yesterday afternoon watching a former co-worker explain a joke I'd once made in Campfire, the software we used for work chats. It wasn't, necessarily, the strangest experience — except that it was occurring in a taped deposition that was being played in court, in the midst of a lawsuit that was being livestreamed on the internet to viewers across the world. My chat joke — and my co-worker John Cook's noble attempt to explain it to a lawyer — are now a matter of public record.

Gawker Media, the company where I used to work, is being sued by the wrestler Terry Bollea (better known as Hulk Hogan) over a 2012 story in which Gawker published a short excerpt from a video showing Bollea having sex with Heather Clem, the wife of Bollea's friend Bubba the Love

Parker Higgins ☂

@xor

Following

Google dev email quoted: "Our [APIs] are half-ass at best. We need another half an ass."

RETWEETS 52 LIKES 80

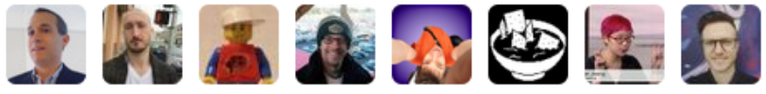
Chris DeSalvo

@chrisdesalvo

Follow

@xor I wrote that. Not sure whether to be embarrassed or to revel in the fact that that is how I'll be immortalized.

LIKES 14



12:00 AM - 11 May 2016

http://money.cnn.com/2015/01/16/technology/security/new-york-post-hacked/

http://money.cnn.com/2015/01/16/technology/security/new-york-post-hacked/

Threat Modeling

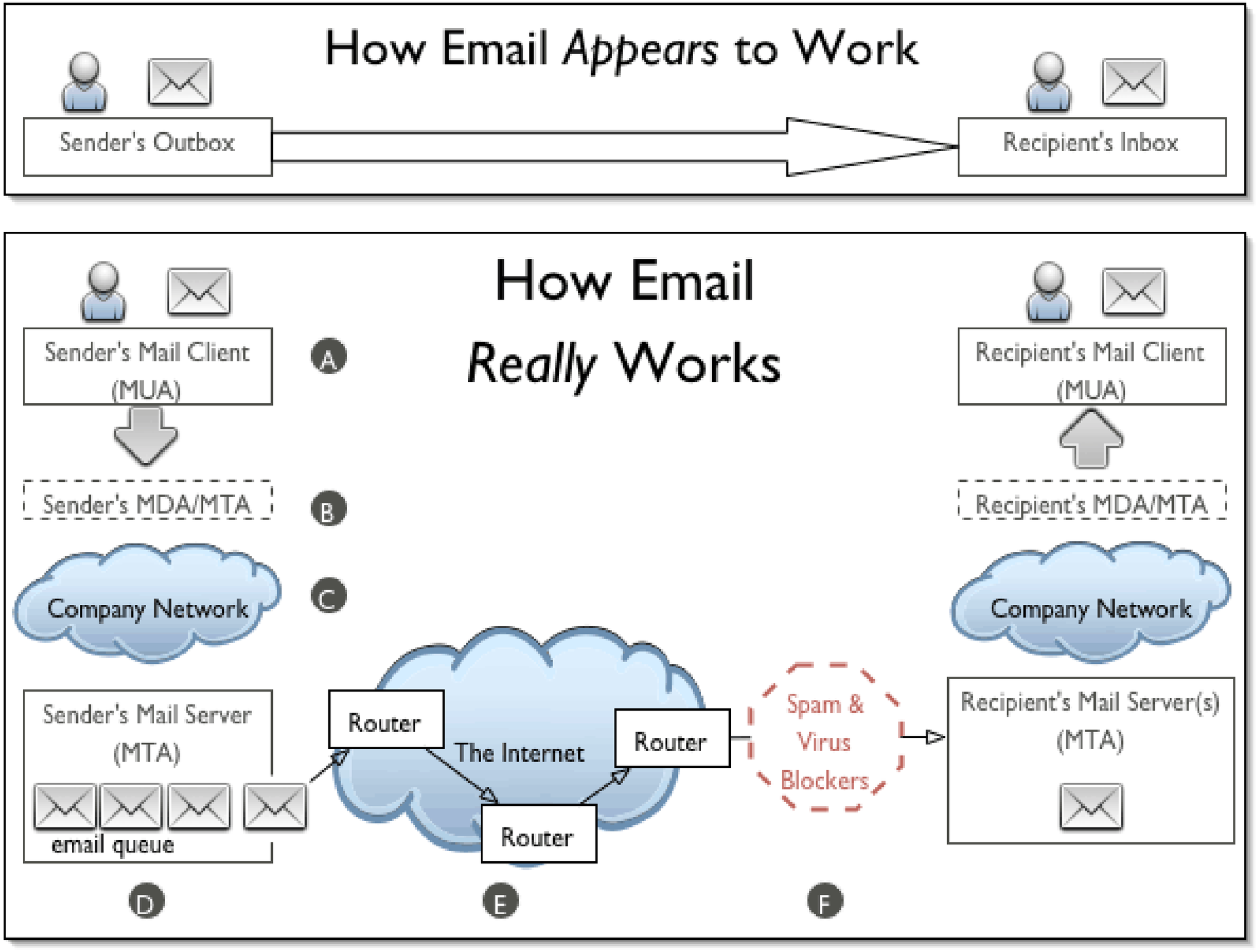
- Basically the who/what/where/when/why/how of thinking about security & risk. Some examples of Qs you might ask:
  - Why might you be targeted?
  - Who are your enemies?
  - What might be used against you?
  - What could go wrong in your day-to-day?
  - How secure do you need it?

https://www.flickr.com/photos/73648871@N00/3023756556/

Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Communication! Calls, messages, files sent; anything out of your hands.



https://www.oasis-open.org/khelp/kmlm/user_help/html/how_email_works.html

http://www.geograph.org.uk/photo/68348

Originating Mail

Destinating Mail

PMPC

PMPC

AMC

AMC

Carrier collection
Mail is picked up from homes, businesses, and mailboxes

Post Office

P&DC

P&DC

Post Office/ DDU

Carrier
Mail is delivered

Window mail
Collected at Post Office or branch

Bulk Standard Mail and Package Services
Standard mail in piece and bulk form

BMEU or DMU
Mail is weighed

HASP

HASP

BMC

First-Class Mail

Priority Mail

Bulk Standard Mail and Package Services

More than one mail type

AMC - Air Mail

BMC - Bulk Mail

BMEU - Business Mail Entry Unit

DDU - Destination Delivery Unit

P&DC - Processing and Distribution Center

PMPC - Priority Mail Processing Center

https://en.wikipedia.org/wiki/Grumman_LLV
https://en.wikipedia.org/wiki/File:USPS_mail_flow_through_national_infrastructure.svg

POST CARD

JERSEY CITY, N.J.
AUG 26
6 30 PM
1911

Dear brother Arthur
So Glad you are
having a good
time and enjoying
but we will all
be glad to see you
again We all rec'd
your postals to-day
from
Ralph

love
&
kisses.

mr A. Freudenberg.
% Laurences Cottage
Highlands
New Jersey.

Box 84

PRINTED IN GERMANY.

https://en.wikipedia.org/wiki/File:Freudenberg_ArthurOscar_02.jpg

https://commons.wikimedia.org/wiki/File:Airmail_envelope_from_Kabala,_Sierra_Leone_%28West_Africa%29_to_Portland,_Oregon_%28USA%29_%283710984093%29.jpg

Teen Dating Site Left Underage Users' Private Messages Exposed To Anyone

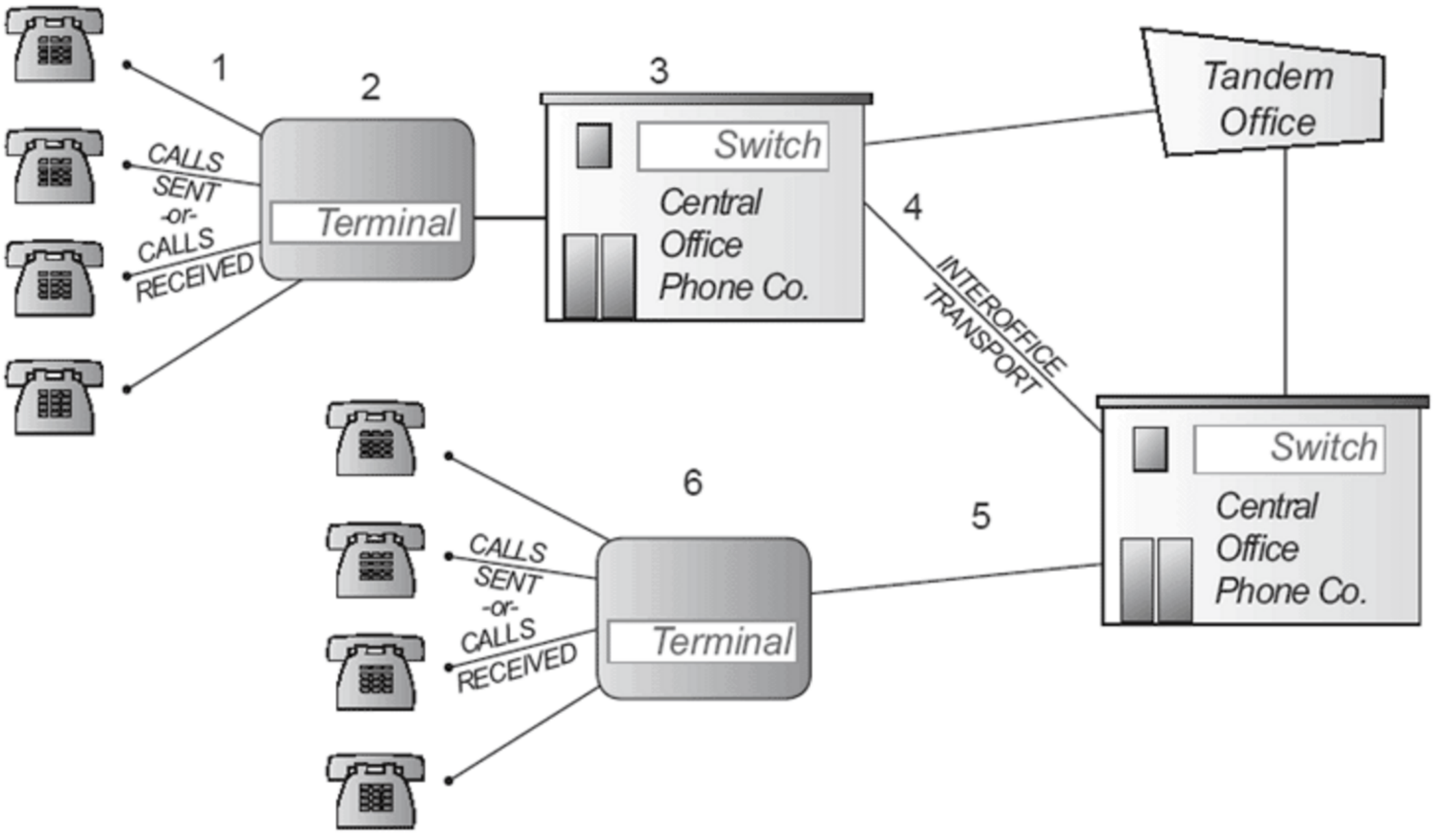
Written by **LORENZO FRANCESCHI-BICCHIERAI**

May 11, 2016 // 01:02 PM EST

The youth dating site OurTeenNetwork claims to be the "best rated teen dating and social networking site," created "for the safety of online teen dating and socializing." But despite those hefty claims and promises, until this week, anyone on the internet could read the private messages exchanged between users, and even impersonate them.

All you had to do snoop on anyone's conversations was register to the site, and then guess a user's unique identification number. As chance would have it, that wasn't very hard at all.

Plain Old Telephone Service (POTS) Networking

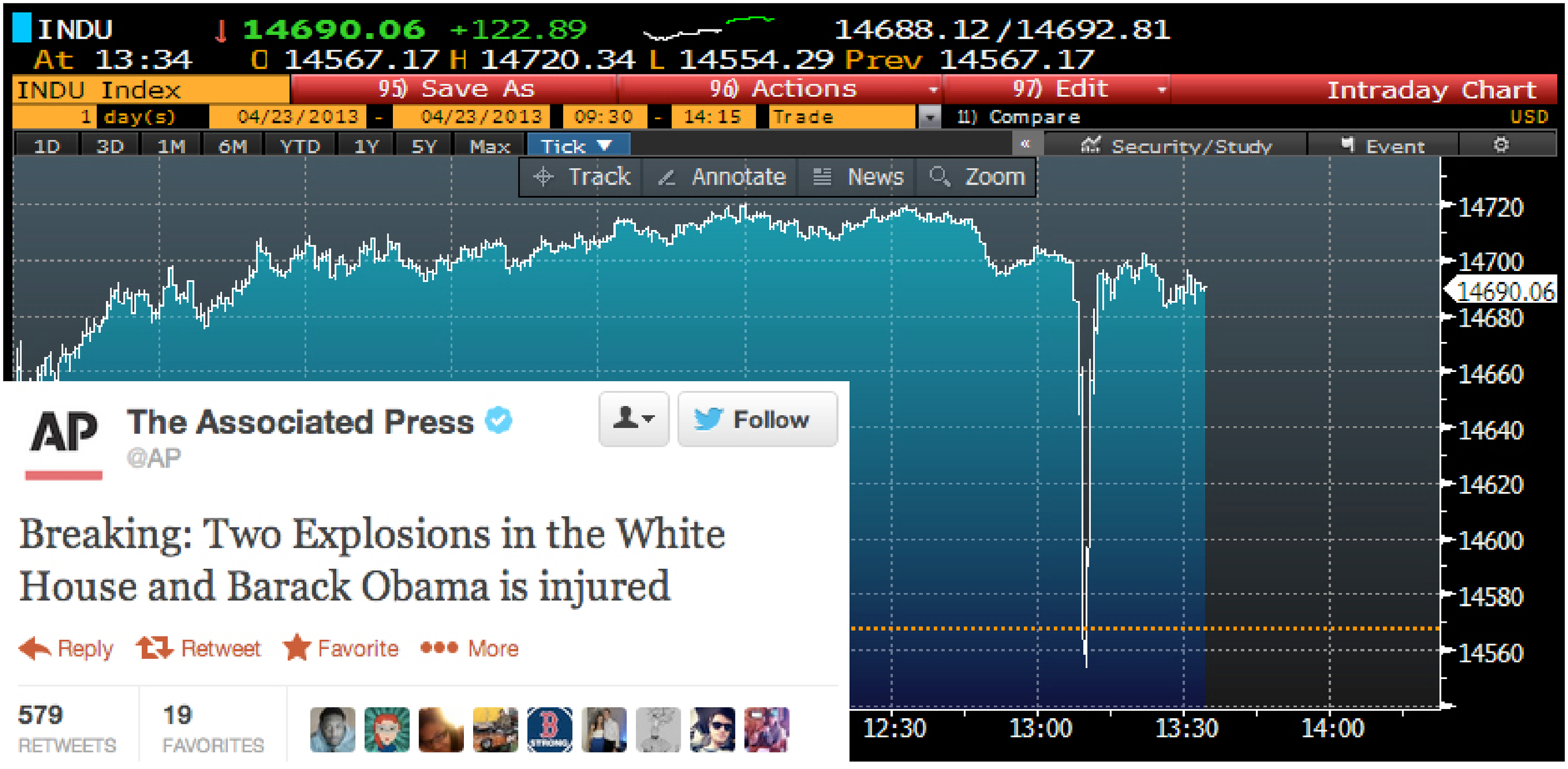


https://www.mackinac.org/6765

Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Communication! Calls, messages, files sent; anything out of your hands.

Metadata. Who are you talking to & when. How big are those files/msgs?



http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

http://www.salon.com/2013/04/24/how_a_twitter_hack_sent_the_market_plummeting_ap/

Data at rest. What's on your computer? What's sitting in your e-mail archive?

Data in motion. Calls, messages, files sent; anything out of your hands.

Metadata. Who are you talking to & when. How big are those files/msgs?

Identities & logins.

Help is on the way

Mobile tools: Secure calling and messaging

Web browsing:

- More encryption & malware blocking.
- Anonymous browsing

Messaging: Secure chats and video calls

E-mail & file encryption

Software updates

Security holes in Windows, Mac, and Linux, are discovered on a near-daily basis. Same with browsers and most other software.

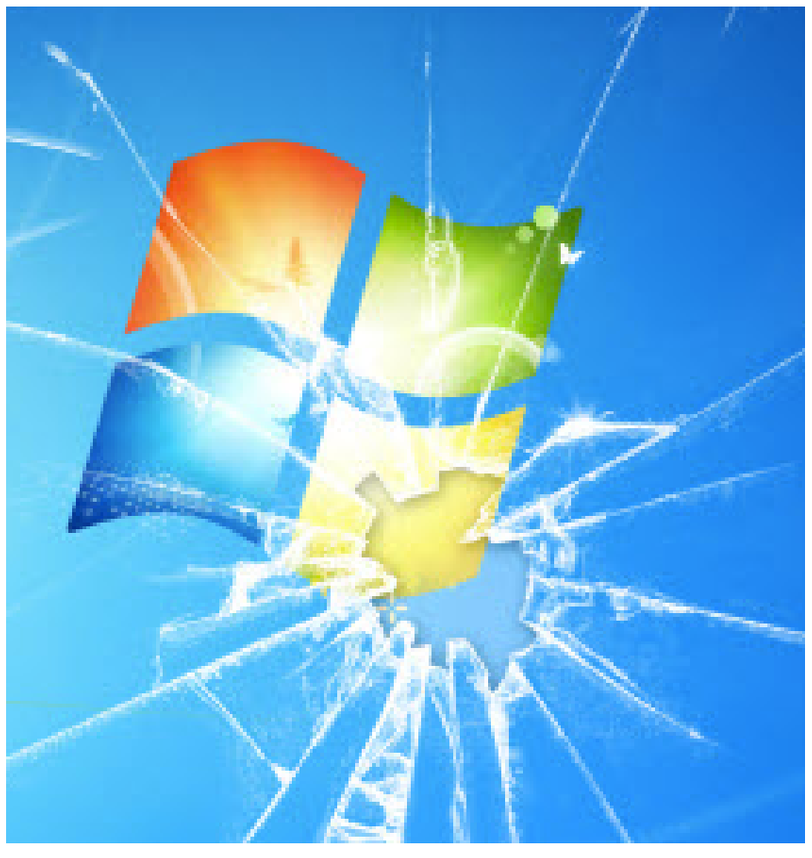
(When it annoys you to restart & update, just do it!)

10 Adobe, Microsoft Push Critical Updates

MAY 16

Adobe has issued security updates to fix weaknesses in its **PDF Reader** and **Cold Fusion** products, while pointing to an update to be released later this week for its ubiquitous **Flash Player** browser plugin. Microsoft meanwhile today released 16 update bundles to address dozens of security flaws in **Windows, Internet Explorer** and related software.

Microsoft's patch batch includes updates for "zero-day" vulnerabilities (flaws that attackers figure out how to exploit before before the software maker does) in Internet Explorer (IE) and in Windows. Half of the 16 patches that Redmond issued today earned its "critical" rating, meaning the vulnerabilities could be exploited remotely through no help from the user, save for perhaps clicking a link, opening a file or visiting a hacked or malicious Web site.



According to security firm **Shavlik**, two of the Microsoft patches tackle issues that were publicly disclosed prior to today's updates, including bugs in IE and the **Microsoft .NET Framework**.

Passwords

Don't use the same couple of passwords everywhere.

Your e-mail password needs to be stronger than your bank's. (At least you can call up your bank for help if there's fraud. Not so much w/e-mail.)

E-mail owns your other accounts — nearly every website has an "I forgot my password" feature that e-mails you.

Passwords

An 8 letter password with numbers and symbols can be cracked in a few days, but an 8 word phrase could take centuries.

"Pass phrases" – use a real sentence instead of just one word. Google and Twitter (& many others) let you use a password as long as you want!

Unfortunately, websites don't always let you do this.

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

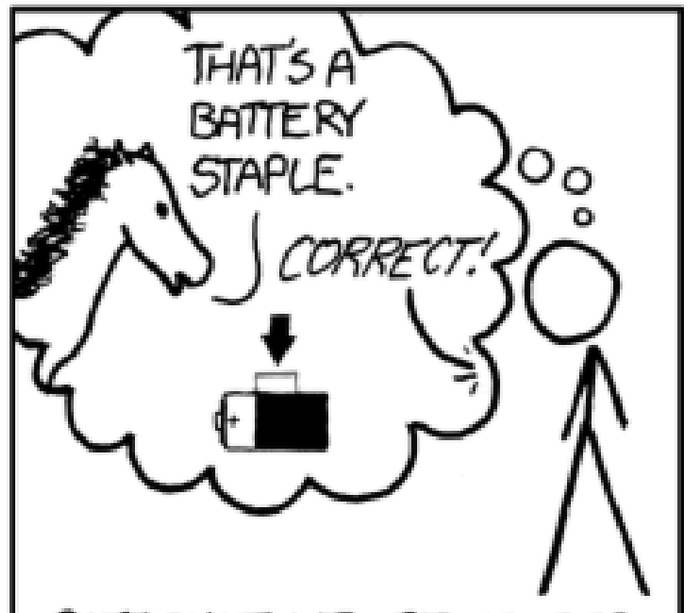
FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

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

DIFFICULTY TO GUESS:

HARD



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.

https://xkcd.com/936/

Password Managers

Helps you use a different password everywhere. Can generate totally random passwords for every website.

1Password (Mac/iOS/Windows)

LastPass (multiplatform, website)

KeePassX (multiplatform app)

File encryption

- Protects files
- Use case: sending sensitive files or putting files on USB sticks to share.

- TrueCrypt (multiplatform)
- MiniLock (multiplatform)

Full disk encryption

- Protects all data on your computer, when computer is turned off.
- Use case: Protects if computer is stolen

- Apple FileVault (Mac)
- BitLocker (Windows "*Pro*" or "*Enterprise*" versions)

Security & Privacy

Show All

osxdaily.com

General | FileVault | Firewall | Privacy

FileVault secures the data on your disk by encrypting its contents automatically.

Turn On FileVault...

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk "Macintosh HD".

Click the lock to prevent further changes.

Advanced...

?

BitLocker Drive Encryption

« System and Security ▸ BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

- TPM Administration
- Disk Management
- Privacy statement