Better PHP Security
Learning from Adobe

Quickly, about me

Consultant
Senior Engineer
Developer
Senior Developer
Director of Tech
Hosting Manager
Support Tech

columbus php

laravel

DESIGNER VS DEVELOPER

2014: Digital Director

lmg Lunne Marketing Group

Not a Drupal guru.

What Happened?

- October 4th: Adobe admits that attackers accessed their network and all passwords have been reset. They believe 3 million accounts are included.
- November: Account total bumped to 38 million
- November: Account total again bumped to 150 million, and with additional data (names, password hints, etc.), the total file size is 10GB.

Is it significant?

- Adobe listed the data as “encrypted”. Experts stated that this was probably in error and what they really meant is that it was hashed... and the experts were wrong.

- The dataset includes rich plaintext emails, usernames,password hints and encrypted password hashes. Additionally, credit card data was also accessed and is said to use similar encryption.

- Because the frequency of matching password hashes, we know that the data is unsalted and likely uses 3DES.

- No one has publicly announced that they have accessed the private key, however it’s only a matter of time before it’s found.

Why this is a huge problem

- At 150 million accounts, many people will have reused passwords for other sites, and because Adobe uses emails for login, those will most likely match too. (Hello banking/Facebook/etc)?

- Adobe has the credit card data on file for every Creative Cloud customer and people who have purchased other products.

- Once cracked this provides an even better (larger) dataset for commonly used passwords than lists from Gawker and others.

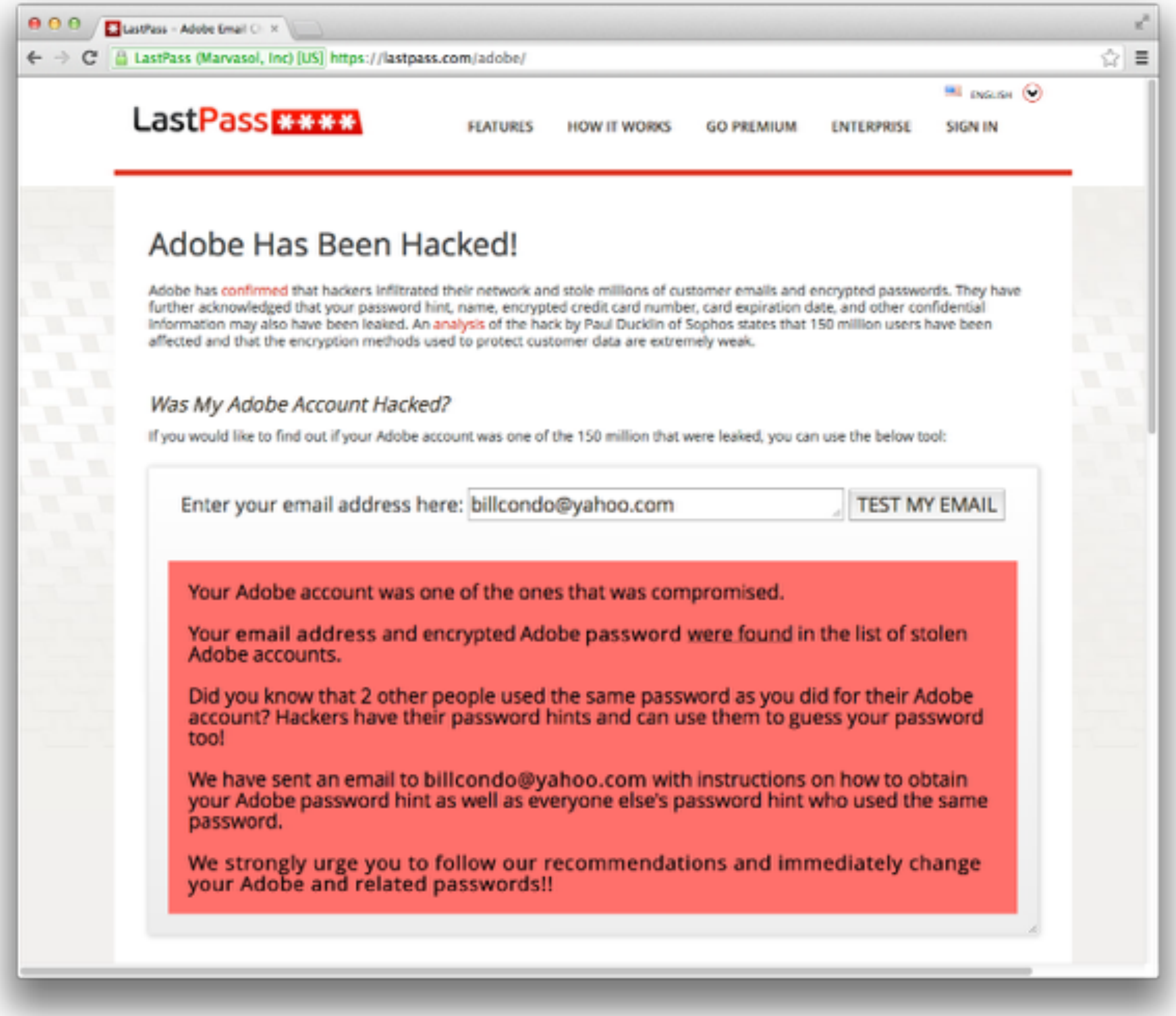
What Adobe did right

- Changing people's passwords
- Hey, at least they didn't store their private key with everything else

What Adobe did wrong

- Encrypting and not hashing passwords
- Not salting passwords
- Storing plain text password hints with the other data
- Allowing poor passwords
- Allowing poor password hints
- Slow response

LastPass: Lookup Tool



Adobe Has Been Hacked!

Adobe has confirmed that hackers infiltrated their network and stole millions of customer emails and encrypted passwords. They have further acknowledged that your password hint, name, encrypted credit card number, card expiration date, and other confidential information may also have been leaked. An analysis of the hack by Paul Ducklin of Sophos states that 150 million users have been affected and that the encryption methods used to protect customer data are extremely weak.

Was My Adobe Account Hacked?

If you would like to find out if your Adobe account was one of the 150 million that were leaked, you can use the below tool:

Enter your email address here: billcondo@yahoo.com TEST MY EMAIL

Your Adobe account was one of the ones that was compromised.

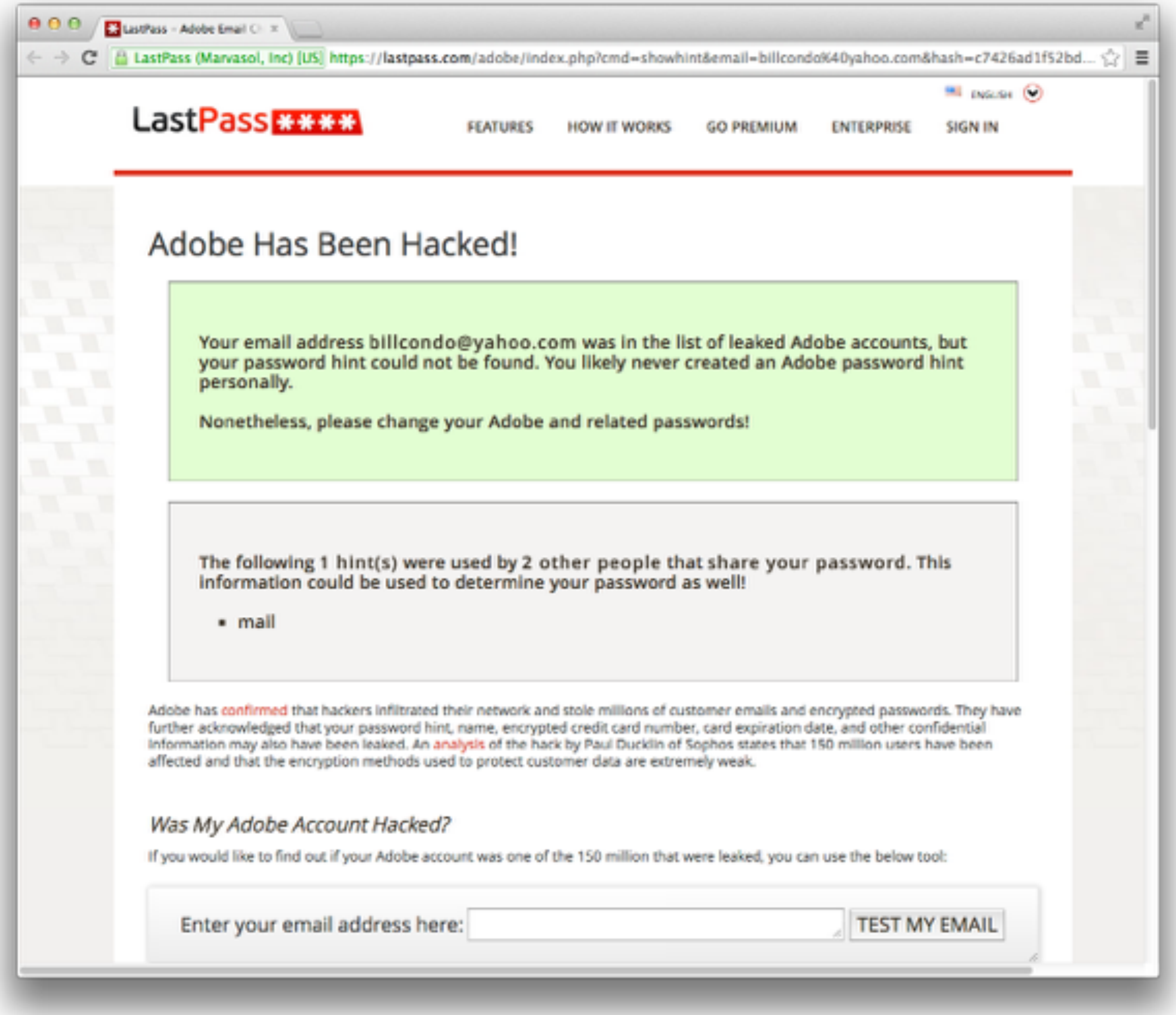
Your email address and encrypted Adobe password were found in the list of stolen Adobe accounts.

Did you know that 2 other people used the same password as you did for their Adobe account? Hackers have their password hints and can use them to guess your password too!

We have sent an email to billcondo@yahoo.com with instructions on how to obtain your Adobe password hint as well as everyone else's password hint who used the same password.

We strongly urge you to follow our recommendations and immediately change your Adobe and related passwords!!

LastPass: Password Hints



LastPass - Adobe Email C
LastPass (Marvasol, Inc) [US]
https://lastpass.com/adobe/index.php?cmd=showhint&email=billcondo%40yahoo.com&hash=c7426ad1f52bd...
LastPass ****
ENGLISH
FEATURES
HOW IT WORKS
GO PREMIUM
ENTERPRISE
SIGN IN

Adobe Has Been Hacked!

Your email address billcondo@yahoo.com was in the list of leaked Adobe accounts, but your password hint could not be found. You likely never created an Adobe password hint personally.

Nonetheless, please change your Adobe and related passwords!

The following 1 hint(s) were used by 2 other people that share your password. This information could be used to determine your password as well!

- mail

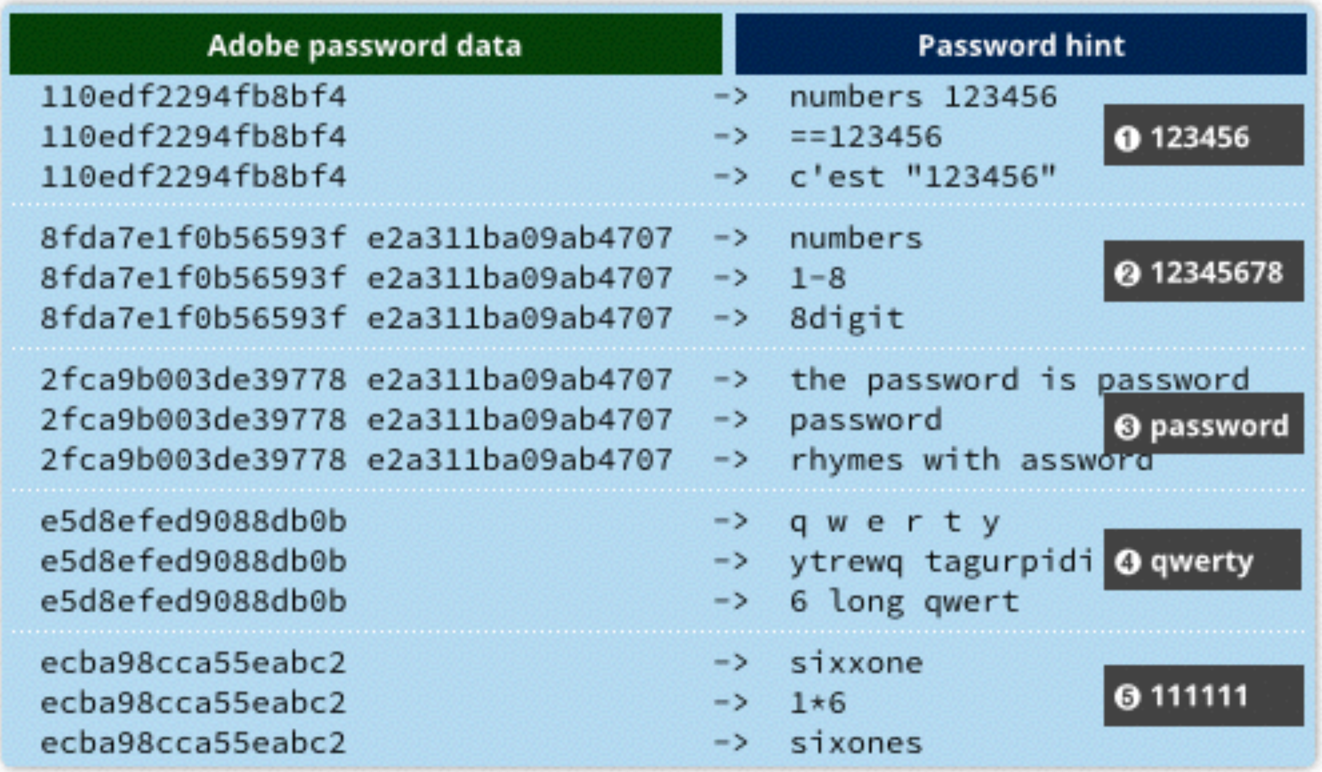
Adobe has confirmed that hackers infiltrated their network and stole millions of customer emails and encrypted passwords. They have further acknowledged that your password hint, name, encrypted credit card number, card expiration date, and other confidential information may also have been leaked. An analysis of the hack by Paul Ducklin of Sophos states that 150 million users have been affected and that the encryption methods used to protect customer data are extremely weak.

Was My Adobe Account Hacked?

If you would like to find out if your Adobe account was one of the 150 million that were leaked, you can use the below tool:

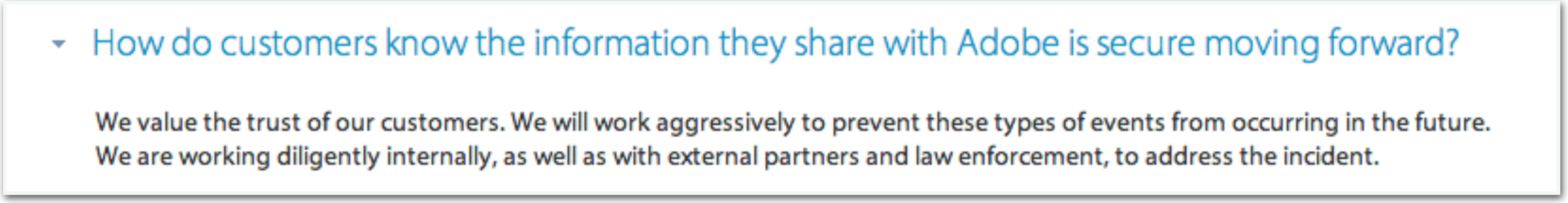
Enter your email address here:

Password Hints



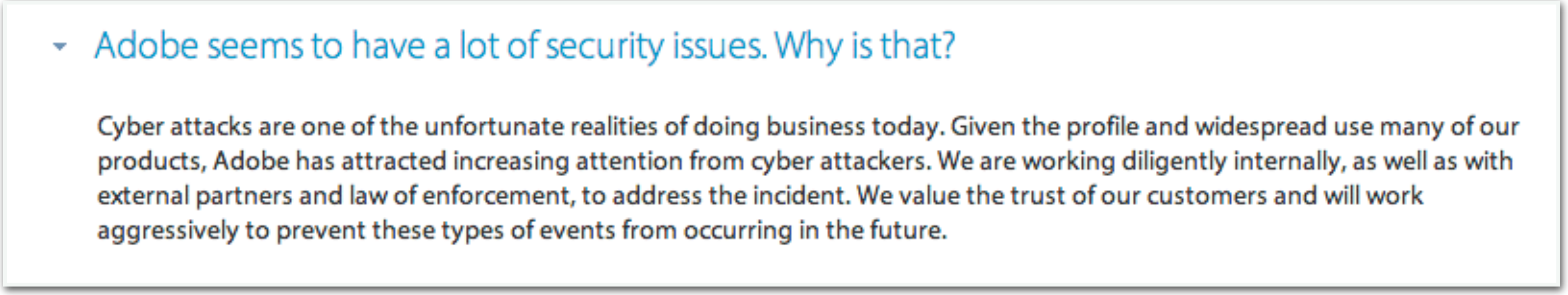
Adobe password data		Password hint	
110edf2294fb8bf4	->	numbers 123456	❶ 123456
110edf2294fb8bf4	->	==123456	
110edf2294fb8bf4	->	c'est "123456"	
8fda7e1f0b56593f e2a311ba09ab4707	->	numbers	❷ 12345678
8fda7e1f0b56593f e2a311ba09ab4707	->	1-8	
8fda7e1f0b56593f e2a311ba09ab4707	->	8digit	
2fca9b003de39778 e2a311ba09ab4707	->	the password is password	❸ password
2fca9b003de39778 e2a311ba09ab4707	->	password	
2fca9b003de39778 e2a311ba09ab4707	->	rhymes with assword	
e5d8efed9088db0b	->	q w e r t y	❹ qwerty
e5d8efed9088db0b	->	ytrewq tagurpidi	
e5d8efed9088db0b	->	6 long qwert	
ecba98cca55eabc2	->	sixxone	❺ 111111
ecba98cca55eabc2	->	1*6	
ecba98cca55eabc2	->	sixones	

Adobe FAQ



How do customers know the information they share with Adobe is secure moving forward?

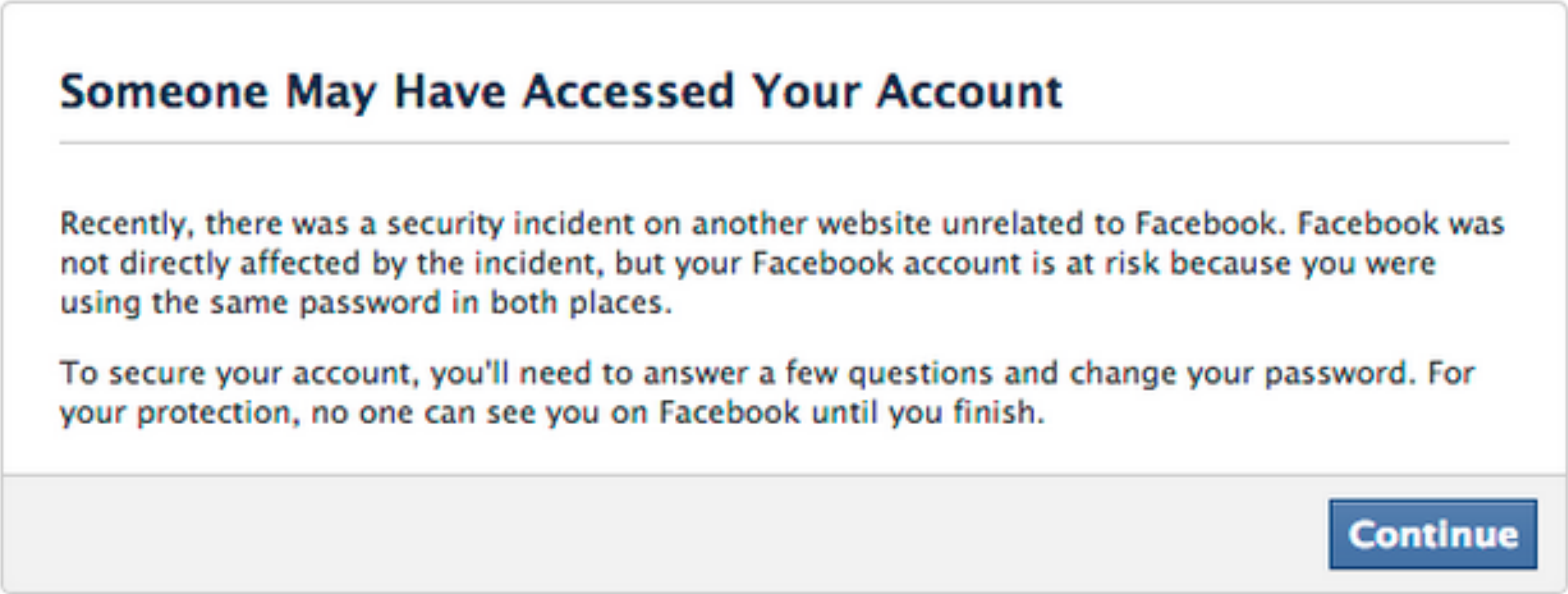
We value the trust of our customers. We will work aggressively to prevent these types of events from occurring in the future. We are working diligently internally, as well as with external partners and law enforcement, to address the incident.



Adobe seems to have a lot of security issues. Why is that?

Cyber attacks are one of the unfortunate realities of doing business today. Given the profile and widespread use many of our products, Adobe has attracted increasing attention from cyber attackers. We are working diligently internally, as well as with external partners and law of enforcement, to address the incident. We value the trust of our customers and will work aggressively to prevent these types of events from occurring in the future.

Facebook's Response

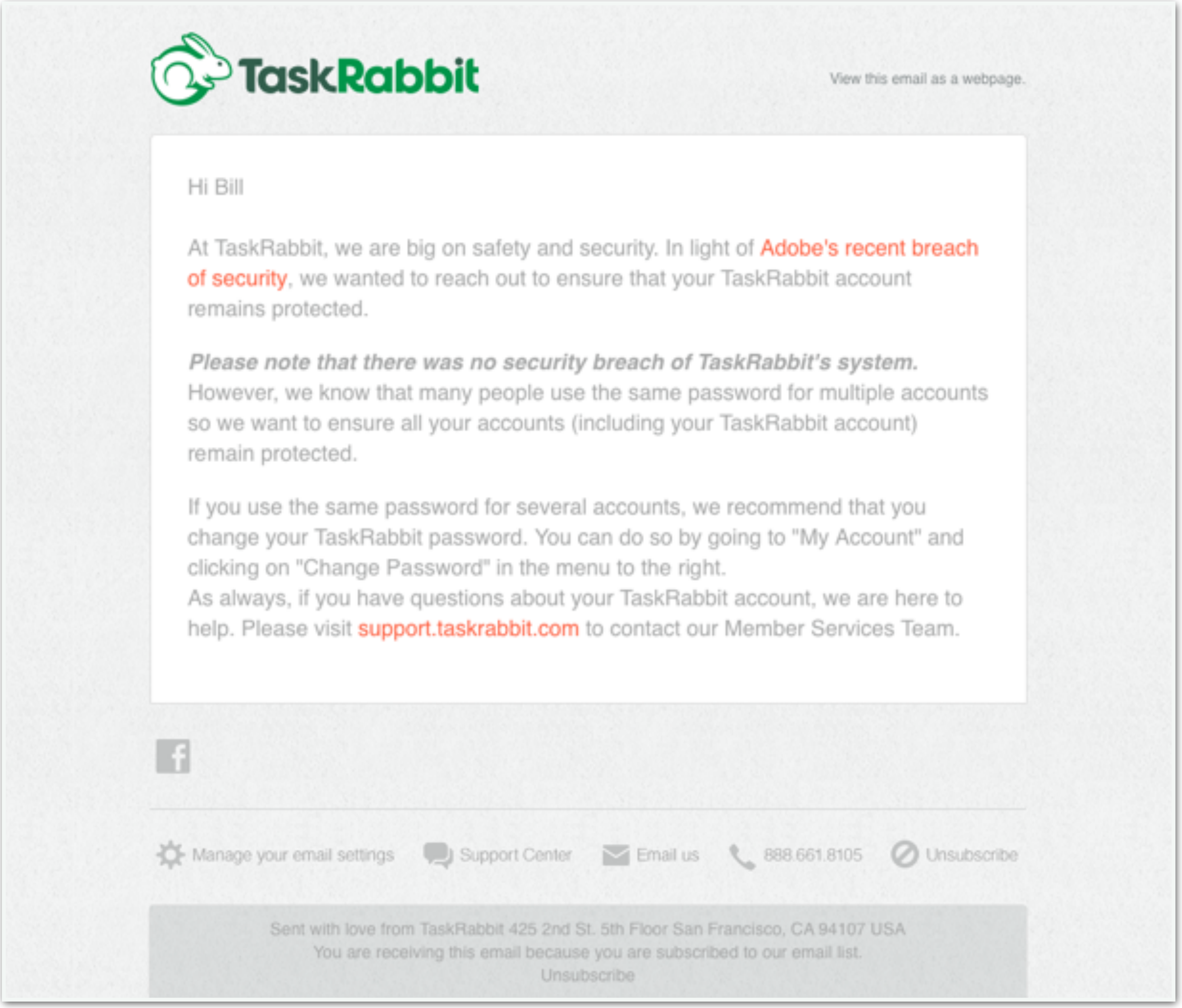


Someone May Have Accessed Your Account

Recently, there was a security incident on another website unrelated to Facebook. Facebook was not directly affected by the incident, but your Facebook account is at risk because you were using the same password in both places.

To secure your account, you'll need to answer a few questions and change your password. For your protection, no one can see you on Facebook until you finish.

TaskRabbit’s Response



TaskRabbit

View this email as a webpage.

Hi Bill

At TaskRabbit, we are big on safety and security. In light of Adobe's recent breach of security, we wanted to reach out to ensure that your TaskRabbit account remains protected.

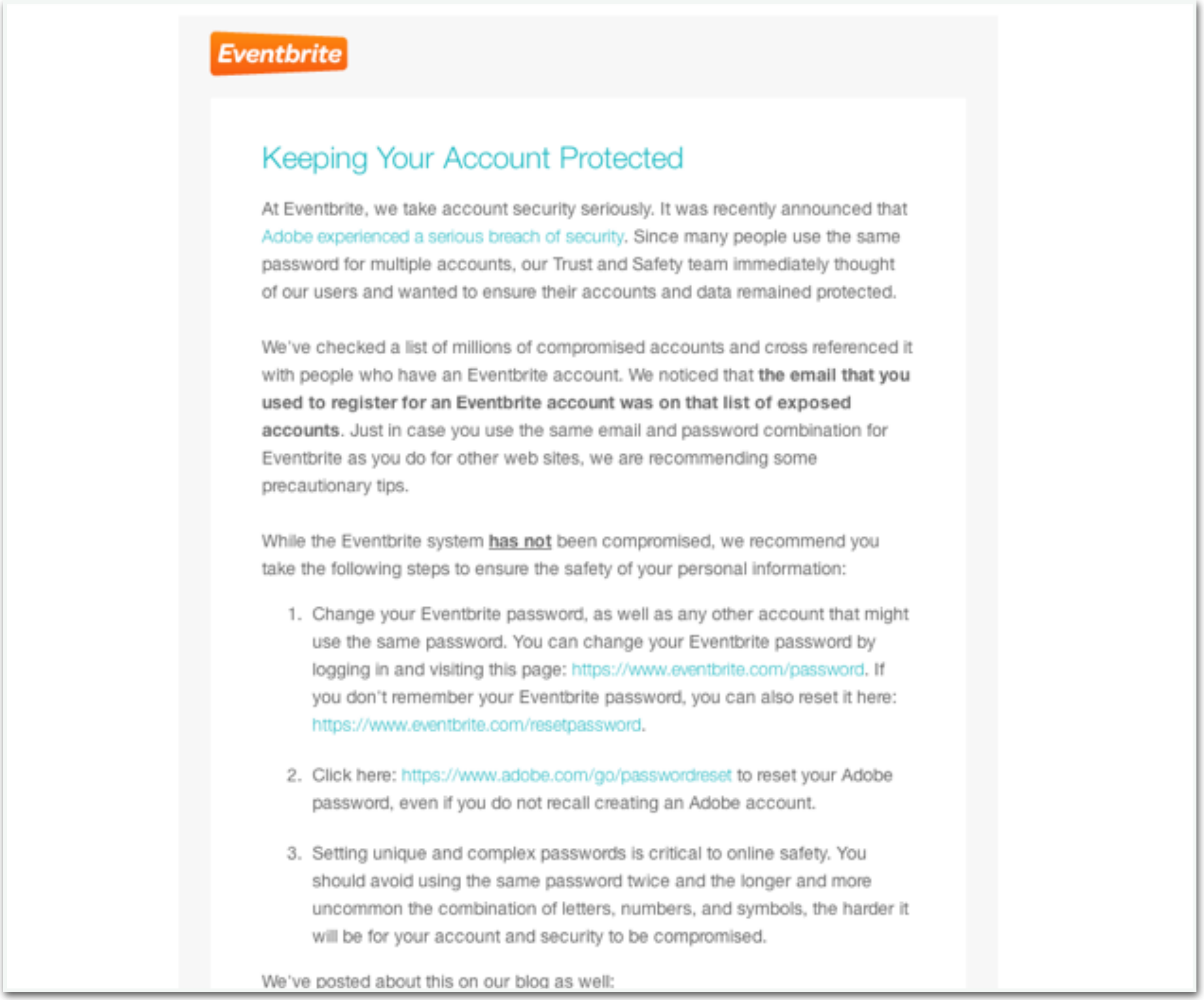
Please note that there was no security breach of TaskRabbit's system. However, we know that many people use the same password for multiple accounts so we want to ensure all your accounts (including your TaskRabbit account) remain protected.

If you use the same password for several accounts, we recommend that you change your TaskRabbit password. You can do so by going to "My Account" and clicking on "Change Password" in the menu to the right.
As always, if you have questions about your TaskRabbit account, we are here to help. Please visit support.taskrabbit.com to contact our Member Services Team.

Manage your email settings · Support Center · Email us · 888.661.8105 · Unsubscribe

Sent with love from TaskRabbit 425 2nd St. 5th Floor San Francisco, CA 94107 USA
You are receiving this email because you are subscribed to our email list.
Unsubscribe

Eventbrite's Response



Keeping Your Account Protected

At Eventbrite, we take account security seriously. It was recently announced that Adobe experienced a serious breach of security. Since many people use the same password for multiple accounts, our Trust and Safety team immediately thought of our users and wanted to ensure their accounts and data remained protected.

We've checked a list of millions of compromised accounts and cross referenced it with people who have an Eventbrite account. We noticed that **the email that you used to register for an Eventbrite account was on that list of exposed accounts**. Just in case you use the same email and password combination for Eventbrite as you do for other web sites, we are recommending some precautionary tips.

While the Eventbrite system **has not** been compromised, we recommend you take the following steps to ensure the safety of your personal information:

1. Change your Eventbrite password, as well as any other account that might use the same password. You can change your Eventbrite password by logging in and visiting this page: https://www.eventbrite.com/password. If you don't remember your Eventbrite password, you can also reset it here: https://www.eventbrite.com/resetpassword.

2. Click here: https://www.adobe.com/go/passwordreset to reset your Adobe password, even if you do not recall creating an Adobe account.

3. Setting unique and complex passwords is critical to online safety. You should avoid using the same password twice and the longer and more uncommon the combination of letters, numbers, and symbols, the harder it will be for your account and security to be compromised.

We've posted about this on our blog as well:

Password Hashing

Things that are fast.

- MD5
- SHA-1
- SHA-256
- SHA-512

… so, don’t use them (alone).

Password Hashing

Things that are slower.

- mcrypt/blowfish
- scrypt

… use mcrypt, consider script in the future.

Passwords in 5.5

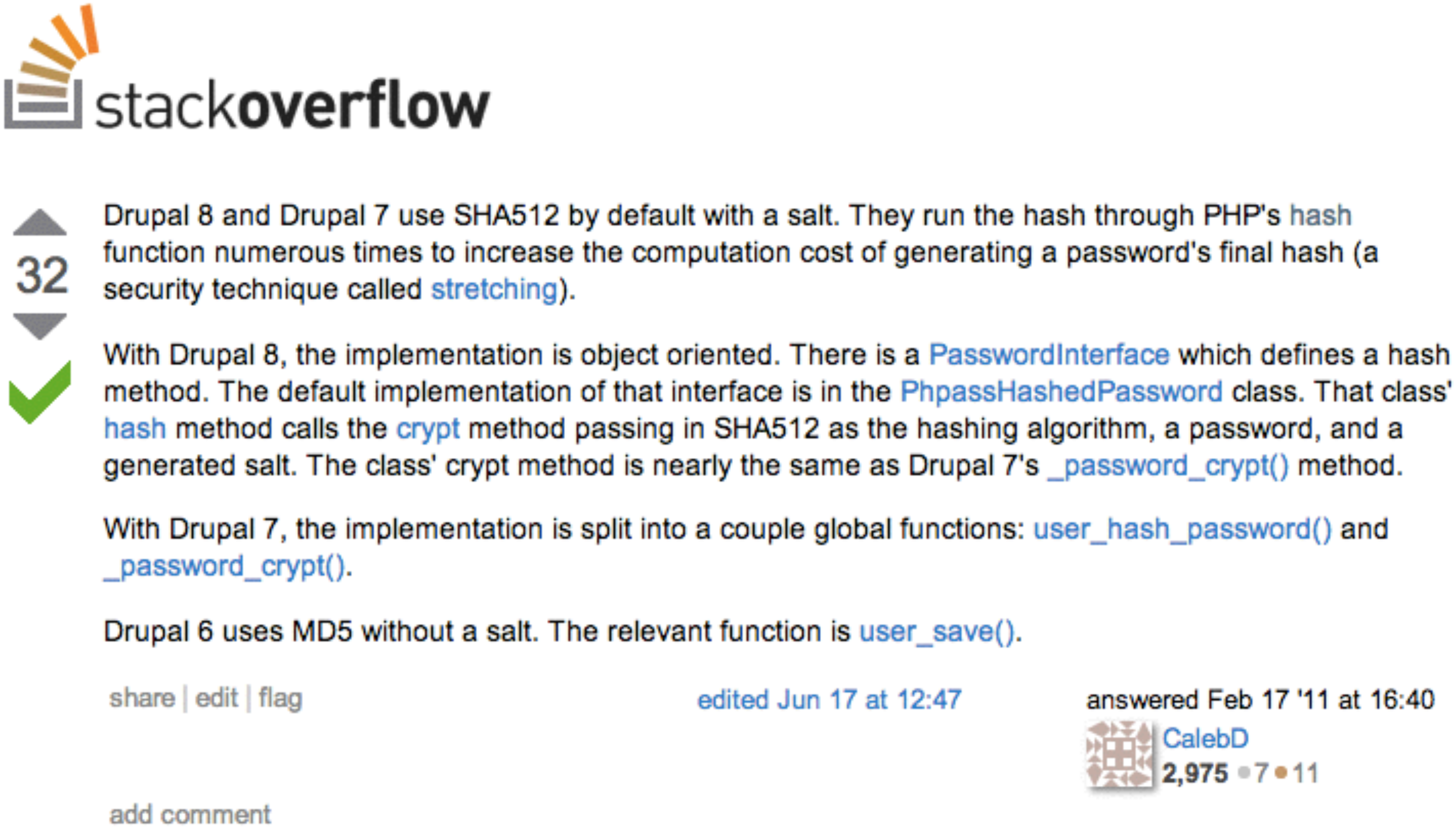
- *string* **password_hash** (string $password , integer $algo [, array $options])
- *boolean* **password_verify** (string $password , string $hash)

Anthony Ferrara

twitter.com/ircmaxell

blog.ircmaxell.com

So, what about Drupal?



Drupal 8 and Drupal 7 use SHA512 by default with a salt. They run the hash through PHP's hash function numerous times to increase the computation cost of generating a password's final hash (a security technique called stretching).

With Drupal 8, the implementation is object oriented. There is a PasswordInterface which defines a hash method. The default implementation of that interface is in the PhpassHashedPassword class. That class' hash method calls the crypt method passing in SHA512 as the hashing algorithm, a password, and a generated salt. The class' crypt method is nearly the same as Drupal 7's _password_crypt() method.

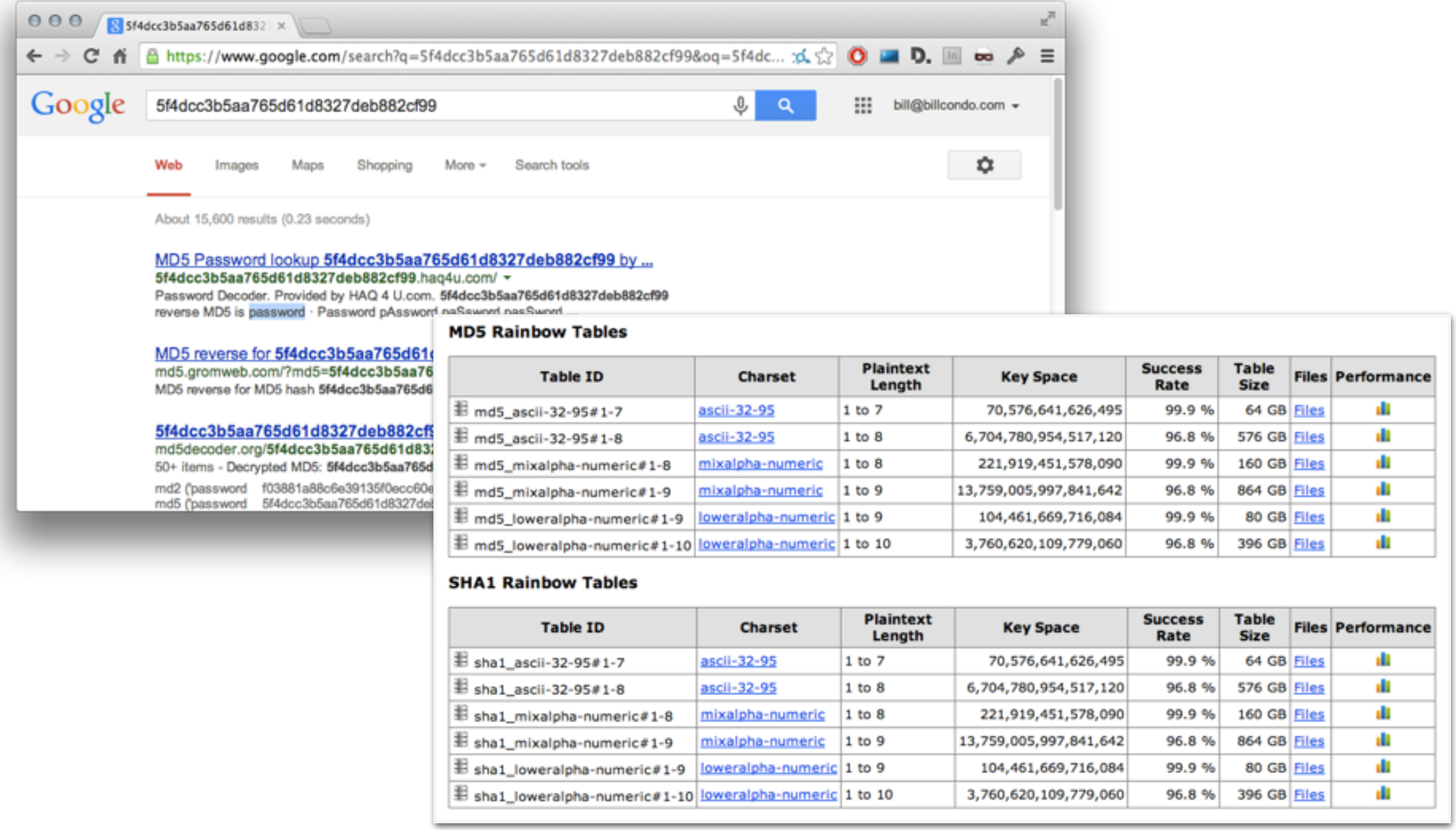
With Drupal 7, the implementation is split into a couple global functions: user_hash_password() and _password_crypt().

Drupal 6 uses MD5 without a salt. The relevant function is user_save().

Quick Note: SALT

- Adds a unique string of characters (hopefully per user) that helps keep the password hashes different for users that have the same password.
- Think about it, without SALT, your password hash may be the same value on ALL of the sites that you use.

Rainbows



5f4dcc3b5aa765d61d832
https://www.google.com/search?q=5f4dcc3b5aa765d61d8327deb882cf99&oq=5f4dc...
Google
5f4dcc3b5aa765d61d8327deb882cf99
bill@billcondo.com
Web
Images
Maps
Shopping
More
Search tools

About 15,600 results (0.23 seconds)

MD5 Password lookup 5f4dcc3b5aa765d61d8327deb882cf99 by ...
5f4dcc3b5aa765d61d8327deb882cf99.haq4u.com/
Password Decoder. Provided by HAQ 4 U.com. 5f4dcc3b5aa765d61d8327deb882cf99
reverse MD5 is password · Password pAssword paSsword pasSword ...

MD5 reverse for 5f4dcc3b5aa765d61
md5.gromweb.com/?md5=5f4dcc3b5aa76
MD5 reverse for MD5 hash 5f4dcc3b5aa765d6

5f4dcc3b5aa765d61d8327deb882cf
md5decoder.org/5f4dcc3b5aa765d61d83
50+ items - Decrypted MD5: 5f4dcc3b5aa765d
md2 ('password f03881a88c6e39135f0ecc60
md5 ('password 5f4dcc3b5aa765d61d8327de

MD5 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
md5_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	64 GB	Files	📊
md5_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	576 GB	Files	📊
md5_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	160 GB	Files	📊
md5_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	864 GB	Files	📊
md5_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	80 GB	Files	📊
md5_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	396 GB	Files	📊

SHA1 Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
sha1_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	64 GB	Files	📊
sha1_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	576 GB	Files	📊
sha1_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	160 GB	Files	📊
sha1_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,997,841,642	96.8 %	864 GB	Files	📊
sha1_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	80 GB	Files	📊
sha1_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,760,620,109,779,060	96.8 %	396 GB	Files	📊

Garbage in, garbage out

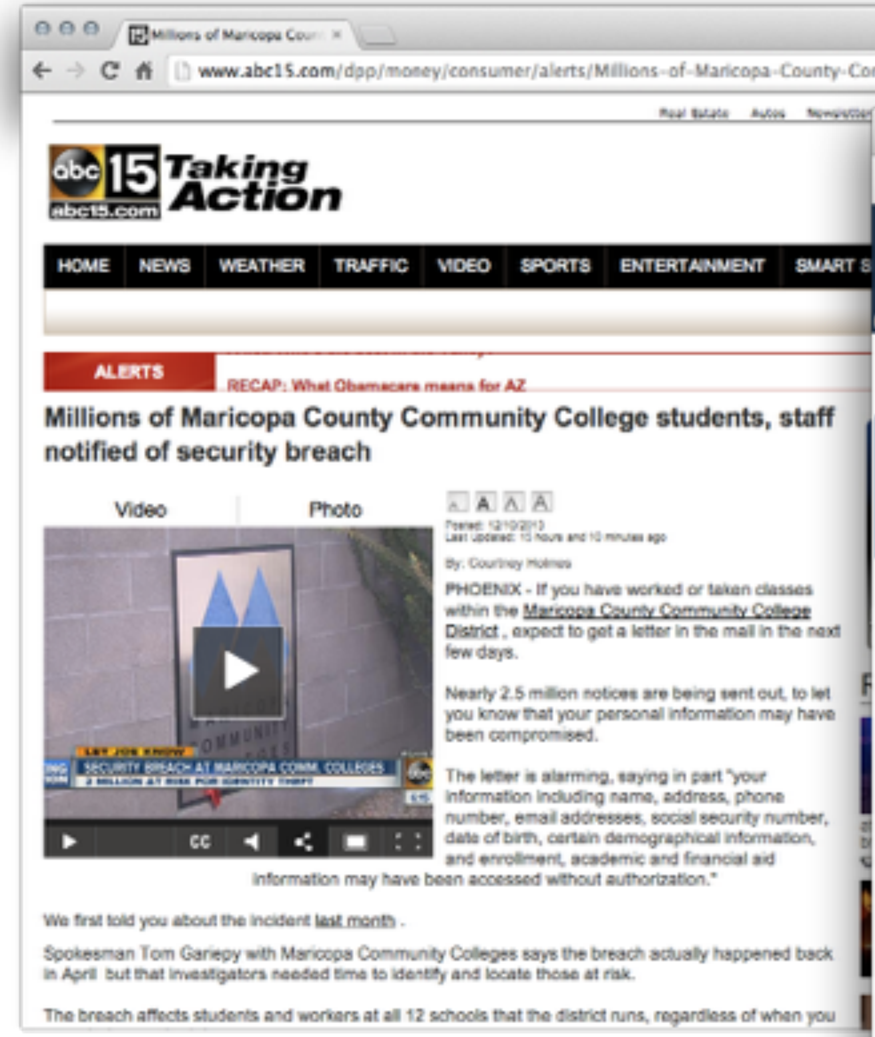
- Having no password policy at all.
- Allowing common passwords like ‘password’, ‘123456’.
- Allowing common dictionary words.

Don’t help the enemy

- Policies that enforce things such as “first character must by upper case” and “must end in a special character”. Allows masking.
- To an extent, disclosing the minimum requirements for lower case, upper case, numeric, and special characters.

Arguments for Password Security

#1 Prevent PR Issues


Millions of Maricopa Coun
www.abc15.com/dpp/money/consumer/alerts/Millions-of-Maricopa-County-Community...
Real Estate
Autos
Newsletter
abc 15 abc15.com
Taking Action
HOME
NEWS
WEATHER
TRAFFIC
VIDEO
SPORTS
ENTERTAINMENT
SMART S
ALERTS
Video
Photo
SECURITY BREACH AT MARICOPA COMM. COLLEGES
CC

RECAP: What Obamacare means for AZ

Millions of Maricopa County Community College students, staff notified of security breach

Posted: 12/10/2013
Last Updated: 10 hours and 10 minutes ago

By: Courtney Holmes

PHOENIX - If you have worked or taken classes within the Maricopa County Community College District , expect to get a letter in the mail in the next few days.

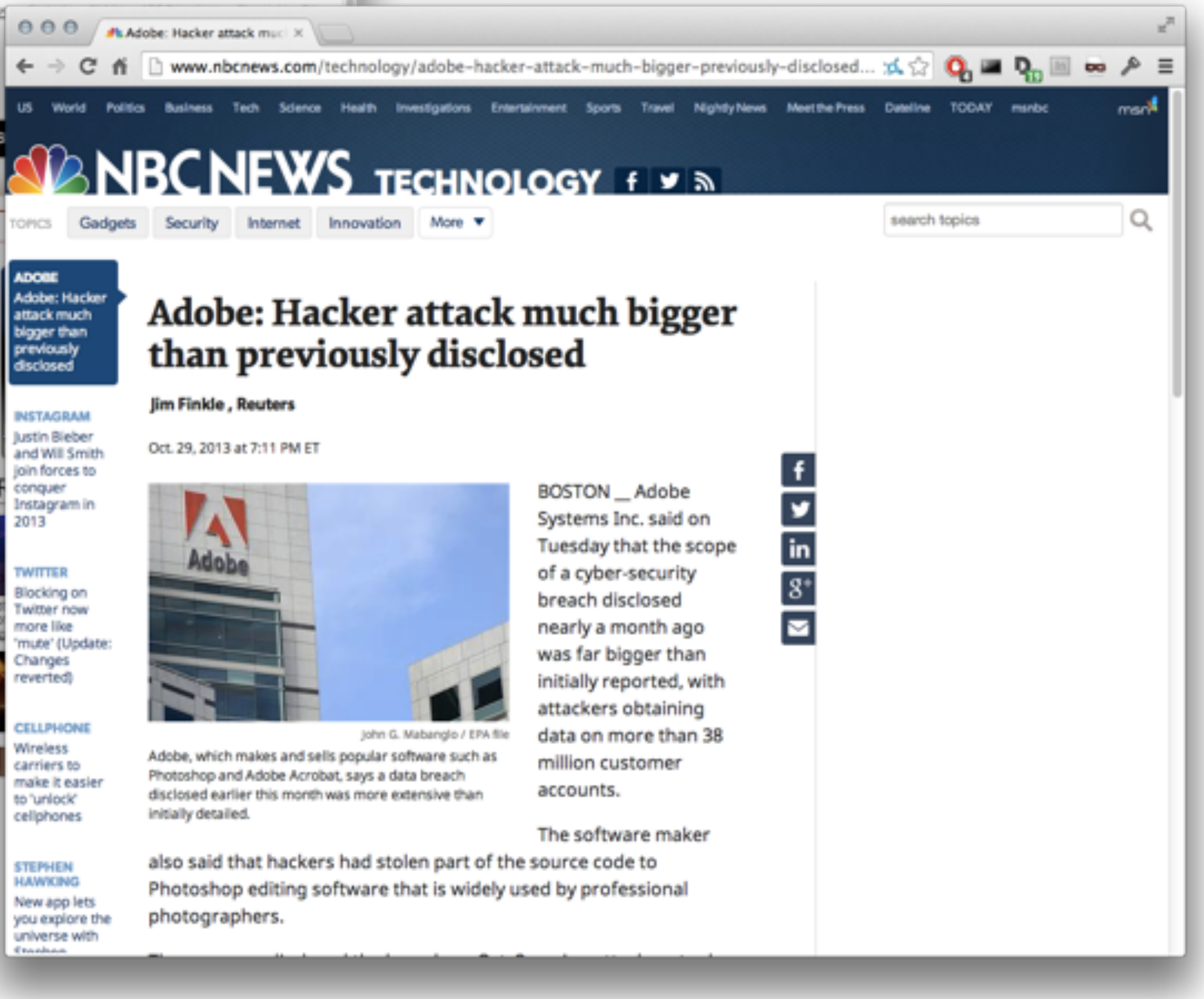
Nearly 2.5 million notices are being sent out, to let you know that your personal information may have been compromised.

The letter is alarming, saying in part "your information including name, address, phone number, email addresses, social security number, date of birth, certain demographical information, and enrollment, academic and financial aid information may have been accessed without authorization."

We first told you about the incident last month .

Spokesman Tom Gariepy with Maricopa Community Colleges says the breach actually happened back in April but that investigators needed time to identify and locate those at risk.

The breach affects students and workers at all 12 schools that the district runs, regardless of when you


Adobe: Hacker attack mu
www.nbcnews.com/technology/adobe-hacker-attack-much-bigger-previously-disclosed...
US
World
Politics
Business
Tech
Science
Health
Investigations
Entertainment
Sports
Travel
Nightly News
Meet the Press
Dateline
TODAY
msnbc
msn
NBC NEWS TECHNOLOGY
TOPICS
Gadgets
Security
Internet
Innovation
More
search topics
ADOBE
Adobe: Hacker attack much bigger than previously disclosed
INSTAGRAM
Justin Bieber and Will Smith join forces to conquer Instagram in 2013
TWITTER
Blocking on Twitter now more like 'mute' (Update: Changes reverted)
CELLPHONE
Wireless carriers to make it easier to 'unlock' cellphones
STEPHEN HAWKING
New app lets you explore the universe with Stephen
Adobe

Adobe: Hacker attack much bigger than previously disclosed

Jim Finkle , Reuters

Oct. 29, 2013 at 7:11 PM ET

John G. Mabanglo / EPA file

Adobe, which makes and sells popular software such as Photoshop and Adobe Acrobat, says a data breach disclosed earlier this month was more extensive than initially detailed.

BOSTON __ Adobe Systems Inc. said on Tuesday that the scope of a cyber-security breach disclosed nearly a month ago was far bigger than initially reported, with attackers obtaining data on more than 38 million customer accounts.

The software maker also said that hackers had stolen part of the source code to Photoshop editing software that is widely used by professional photographers.

#2 Cost vs Risk

- Doing security correctly is less expensive upfront. The opportunity cost is minimal compared the reduction in risk. Cost * Risk = Likelihood Cost
- What does it cost to cleanup the mess: reset the passwords, scan the servers, added support calls/requests, etc…

#3 Predictability

- Help project/business managers in being able to minimize unexpected security response events.
- Better understand how your week is going to go.

Summary

- Store passwords with a good hash, and a unique user-level salt.
- Enforce password rules correctly.
- Be aware of the breaches of other sites.
- Know how to justify good security to management.

Thanks

- @mavrck
    - I'm shameless: I want @mavrck back next year to talk about #drupalcampohio
- slideshare.net/billcondo
- billcondo@gmail.com