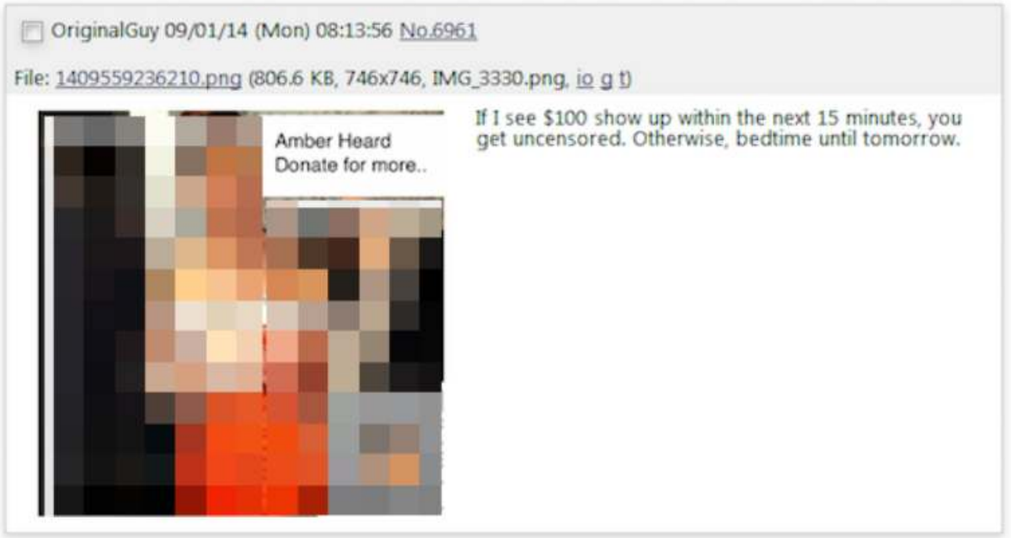
BY BASTIEN AND THEO

WHAT HAPPENED?

31th August 2014

500+ celebrity nude photos leaked

AnonIB and then 4chan



Multiple hackers

> *“ the result of several months of long and hard work*

Different sources, not only iCloud

Released a week before iPhone 6 and iWatch

WHY "ICLOUD" LEAK?

Picture Roll backups are enabled by default

iPhone is a popular platform

BUT, HOW?

BUT, HOW?

Security breach in iCloud!

BUT, HOW?

~~Security breach in iCloud!~~

BUT, HOW?

~~Security breach in iCloud!~~

iCloud API brute-force!

BUT, HOW?

~~Security breach in iCloud!~~

~~iCloud API brute-force!~~

BUT, HOW?

~~Security breach in iCloud!~~

~~iCloud API brute-force!~~

Targeted phishing attacks

BUT, HOW?

~~Security breach in iCloud!~~

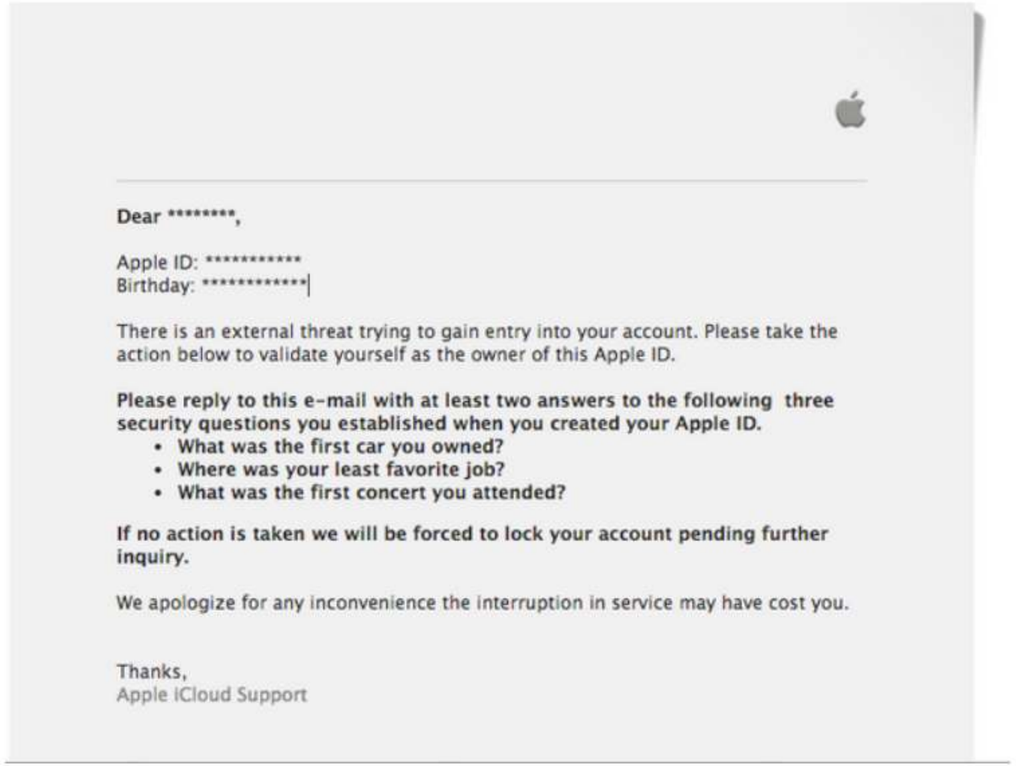
~~iCloud API brute-force!~~

Targeted phishing attacks 

Good old phishing attack...

Good old phishing attack...

ATTACK VECTOR



Dear ********,

Apple ID: **********
Birthday: **********

There is an external threat trying to gain entry into your account. Please take the action below to validate yourself as the owner of this Apple ID.

Please reply to this e-mail with at least two answers to the following three security questions you established when you created your Apple ID.

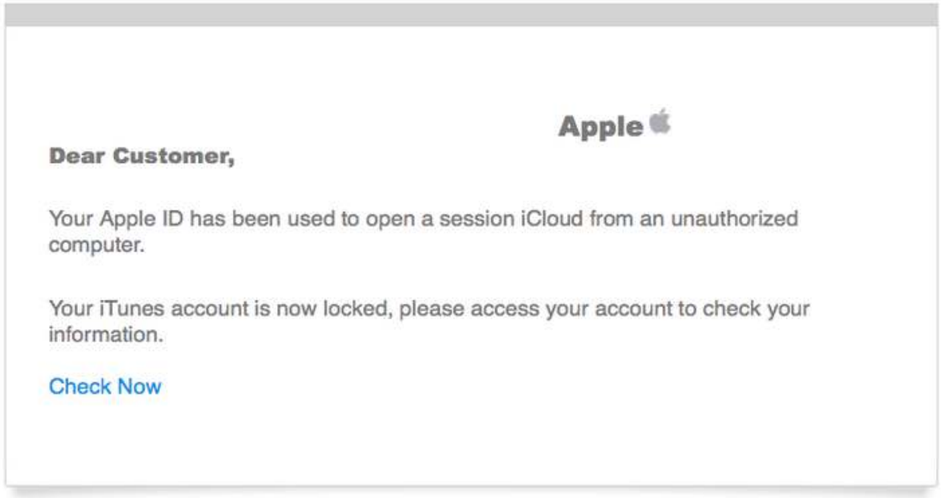
- **What was the first car you owned?**
- **Where was your least favorite job?**
- **What was the first concert you attended?**

If no action is taken we will be forced to lock your account pending further inquiry.

We apologize for any inconvenience the interruption in service may have cost you.

Thanks,
Apple iCloud Support

appleprivacysecurity@gmail.com



Apple

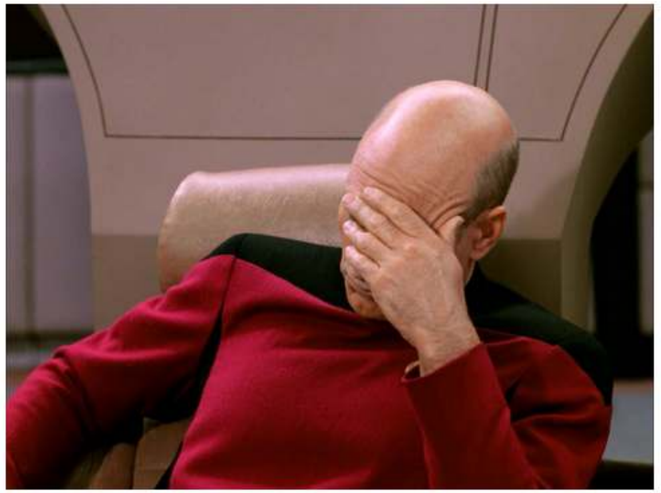
Dear Customer,

Your Apple ID has been used to open a session iCloud from an unauthorized computer.

Your iTunes account is now locked, please access your account to check your information.

Check Now

WEAKNESSES?



Apple ID must:

- Be a valid email address
- Be available
- Not use a domain owned by Apple

ress as your Apple I is will be used as th
ır account.

Please verify your birth date to continue.

Month | Day | Year

Please answer your security questions.

Who was your favorite teacher?

Where were you on January 1, 2000?

WHAT ELSE?


Find My iPhone
●○○○○ Билайн
12:30
Найти iPhone
Apple ID example@icloud.com
Пароль обязательно
Забыли Apple ID или пароль?
NO COUNTERS
NO LOCKERS
NO NOTIFICATION
Инструкции по настройке


nik cubrilovic
@nikcub
Follow
posting an email address as JSON to appleid.apple .com /account/validation /appleid returns if it is a valid account or not. no rate limit.
11:03 AM - 2 Sep 2014


hackappcom / ibrute
Watch 172
Star 1,129
Fork 430

PRESS RELEASE
SEPTEMBER 2, 2014

Apple Media Advisory

Update to Celebrity Photo Investigation

We wanted to provide an update to our investigation into the theft of photos of certain celebrities. When we learned of the theft, we were outraged and immediately mobilized Apple's engineers to discover the source. Our customers' privacy and security are of utmost importance to us. After more than 40 hours of investigation, we have discovered that certain celebrity accounts were compromised by a very targeted attack on user names, passwords and security questions, a practice that has become all too common on the Internet. None of the cases we have investigated has resulted from any breach in any of Apple's systems including iCloud® or Find my iPhone. We are continuing to work with law enforcement to help identify the criminals involved.

To protect against this type of attack, we advise all users to always use a strong password and enable two-step verification. Both of these are addressed on our website at http://support.apple.com/kb/ht4232.

CRISIS MANAGEMENT

Quick response

Working directly with celebrities

Find my iPhone patched in 36h

ACTIONS TAKEN

- Use a strong password for your Apple ID
- Make the answers to your security questions hard to guess
- Protect your account with two-factor authentication
- Check for encryption and SSL
- Employee privacy and security policies

https://support.apple.com/en-gb/HT201303

Avoid phishing emails, fake ‘virus‘ alerts,
phony support calls, and other scams

https://support.apple.com/en-gb/HT204759

TECHNOLOGICAL MEASURES

Dear Eric Slivka,

Your Apple ID [redacted] was used to sign in to iCloud via a web browser.

Date and Time: September 8, 2014, 7:02 AM PDT

If you recently signed in to iCloud.com, you can disregard this email.

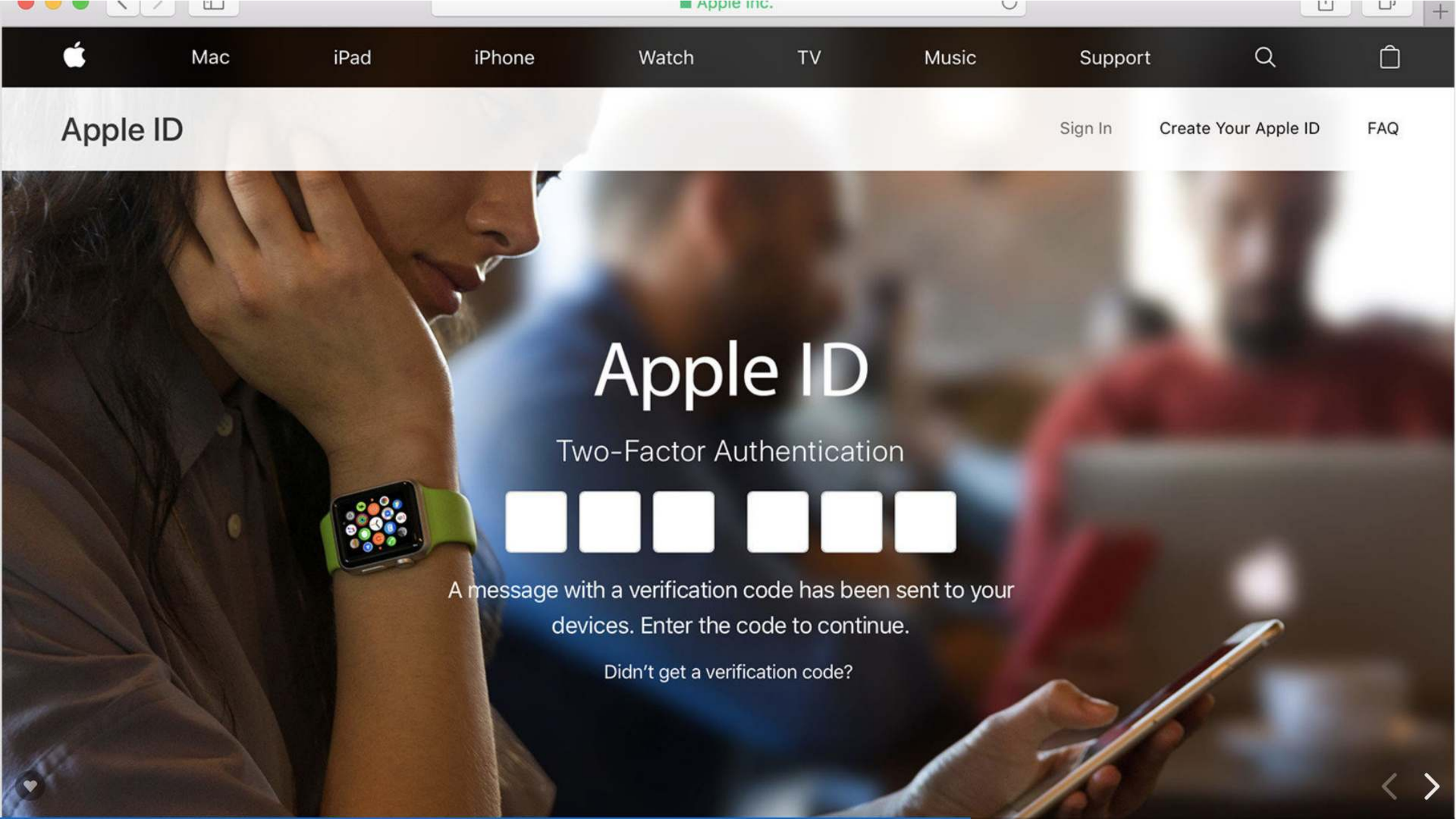
If you have not signed in to iCloud.com recently and believe someone may have accessed your account, you should reset your password at My Apple ID.

Apple Support

User alerting

Hardening

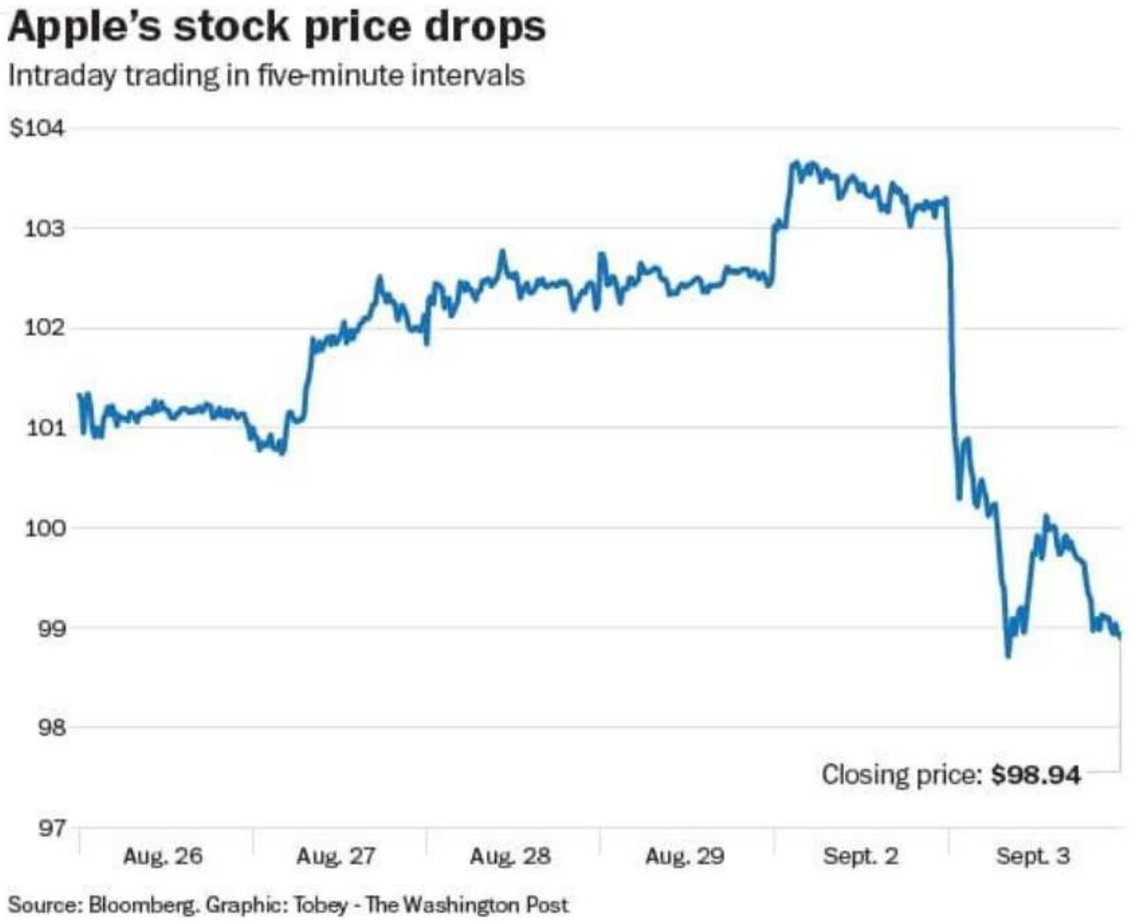
CAPTCHA


Apple Inc.
Mac
iPad
iPhone
Watch
TV
Music
Support
Apple ID
Sign In
Create Your Apple ID
FAQ
Apple ID
Two-Factor Authentication
A message with a verification code has been sent to your devices. Enter the code to continue.
Didn't get a verification code?

REPUTATION COSTS

Remember, one week before iPhone 6 and iWatch

Trust issue



SO MUCH MORE...

Here's what iCloud Backup includes

- App data
- Apple Watch backups
- Call history
- Device settings
- HomeKit configuration
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Photos and videos on your iPhone, iPad, and iPod touch[1]
- Purchase history from Apple services, like your music, movies, TV shows, apps, and books[2]
- Ringtones
- Visual Voicemail password (requires the SIM card that was in use during backup)

https://support.apple.com/en-gb/HT207428

Your iPhone, iPad, and iPod touch backup only include information and settings stored on your device. It doesn't include the information already stored in iCloud, like Contacts, Calendars, Bookmarks, Mail, Notes, shared photos, iCloud Photo Library, My Photo Stream, Health data, and files you store in iCloud Drive.

But Apple did well

A real business behind: Briand Krebs article

REFERENCES

- Celebrity Photo Leak: Is Poor iCloud Security to Blame?
- Notes on the Celebrity Data Theft
- The FBI Is Now Involved in Hunt for the Celebrity Nude Photo Hacker
- Everything We Know About the Alleged Celeb Nude "Trading Ring" and Leak
- HackApp, ibrute was not involved statement
- Celeb hacker 'on the run'
- Apple stock plunges amid celebrity hacking, ahead of purported iWatch announcement
- justice.gov


WHY INCREASE SECURITY MEASURES
IF PEOPLE CLICK ON RANDOM LINKS
imgflip.com

De : Apple
À : [redacted]
Masquer

Rép : [Summary Report] Reminder: Your password Apple has been successfully reset.(Case ID:[redacted])

aujourd'hui à 21:50

Trouvé(e) dans la boîte Réception de H...

Apple ID

New Summary Order Report

Dear Customer [redacted]@hotmail.fr

For Your Protection your Account is automatically Locked, Our System detected an error on your purchased the following product with Credit Card on iTunes Store :

Product	iTunes Gift Card
Order ID	IGC0182V1294ZT
Date	February 1, 2018, 10:50 pm
Price	$55
Shipp To	Alan Emanuel J92 Elmont Road Valley Stream, NY 11580 USA

Please confirm your Apple ID Account to unlock your account and follow all the security procedures by click the following link:

VERIFY MY ACCOUNT

Our system will automatically disabled your Apple ID account if we do not receive any information longer than 24 hours.

reportphishing@apple.com