Cyber Blackmail Campaign

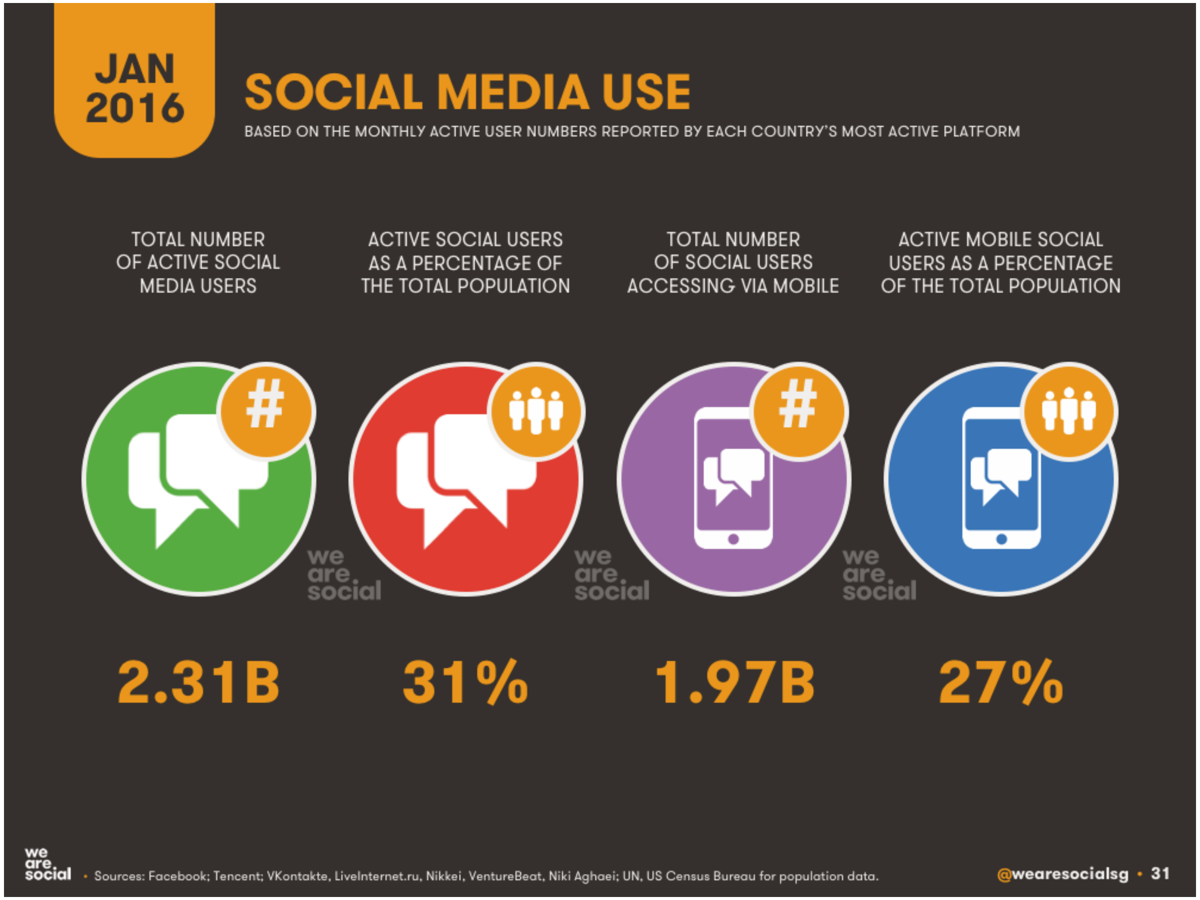
organized by Dubai Police’s Al Ameen Service
in cooperation with the UAE's Telecommunications Regulatory Authority (TRA)

About aeCERT

- The United Arab Emirates Computer Emergency Response Team
- An initiatives of the UAE Telecommunications Regulatory Authority
- Aims at promoting, building and ensuring a safer and secure cyber environment and culture in the UAE

About aeCERT

- aeCERT constituents are:
  - Government & Semi-Government Entities
  - Academic Sector
  - Banking Sector
- Services provided by aeCERT:
  - Monitoring and Response
  - Security Quality Services
  - Awareness and Education



JAN 2016

SOCIAL MEDIA USE

BASED ON THE MONTHLY ACTIVE USER NUMBERS REPORTED BY EACH COUNTRY'S MOST ACTIVE PLATFORM

TOTAL NUMBER OF ACTIVE SOCIAL MEDIA USERS	ACTIVE SOCIAL USERS AS A PERCENTAGE OF THE TOTAL POPULATION	TOTAL NUMBER OF SOCIAL USERS ACCESSING VIA MOBILE	ACTIVE MOBILE SOCIAL USERS AS A PERCENTAGE OF THE TOTAL POPULATION
2.31B	31%	1.97B	27%

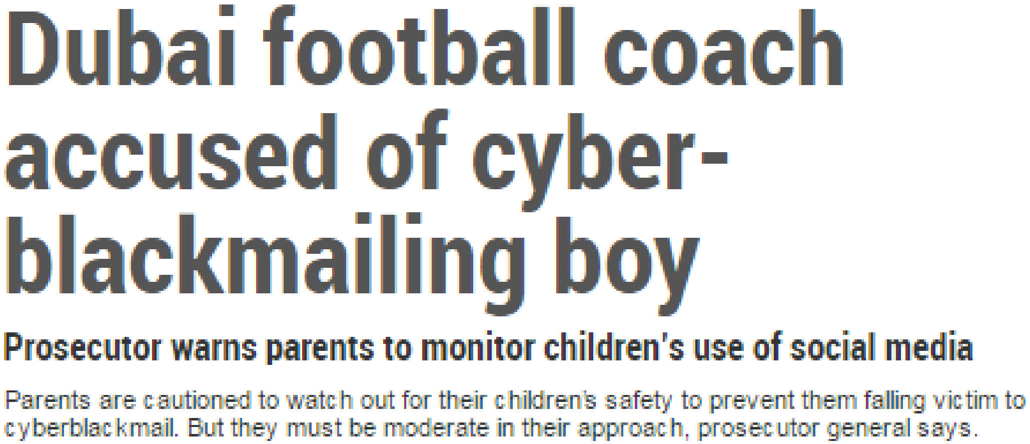
we are social • Sources: Facebook; Tencent; VKontakte, LiveInternet.ru, Nikkei, VentureBeat, Niki Aghaei; UN, US Census Bureau for population data.

@wearesocialsg • 31

http://wearesocial.com/special-reports/digital-in-2016

Cyber Blackmail

The act of threatening to share information about a person to the public, their friends or family, unless a demand is met or money is paid.[1]



Dubai football coach accused of cyber-blackmailing boy

Prosecutor warns parents to monitor children's use of social media

Parents are cautioned to watch out for their children's safety to prevent them falling victim to cyberblackmail. But they must be moderate in their approach, prosecutor general says.

[1] http://www.bbc.co.uk/newsbeat/article/23724703/cyber-blackmail-how-to-keep-safe-and-deal-with-it
http://gulfnews.com/news/uae/courts/dubai-football-coach-accused-of-cyber-blackmailing-boy-1.1703206

شرطة دبي DUBAI POLICE

الأمين al ameen

TRA هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority

Cyber Blackmail Campaign

A collaboration between TRA and Al Ameen Service from Dubai Police, to address the blackmail issue

الابتزاز الإلكتروني
احذر أن تكون التالي..
لاتكن ضحية سهلة
عبر وسائل التواصل الاجتماعي
للإبلاغ
800 4888
الأمين al ameen
خدمة سرية لتوصيل المعلومات
TV

Al Ameen Service

- Al Ameen Service officially launched in September 2003.
- It is a communication channel between public and the General Directorate of State Security.
- People can report any suspicious acts or behaviors in the region confidentially.

Al Ameen Service

- Public can reach the service through
  - toll free telephones, fax & SMS
  - e-mails & website,
  - Social media
  - Al Ameen mobile application

نعمل معاً لإسعادك
TOGETHER for your happiness
Dubai Smart Gov

DUBAI POLICE
al ameen
الابتزاز الإلكتروني
عبر
مواقع التواصل الاجتماعي

du
Blackmail
Beware.. that you are the next
be an easy victim
gh social media
800 4888

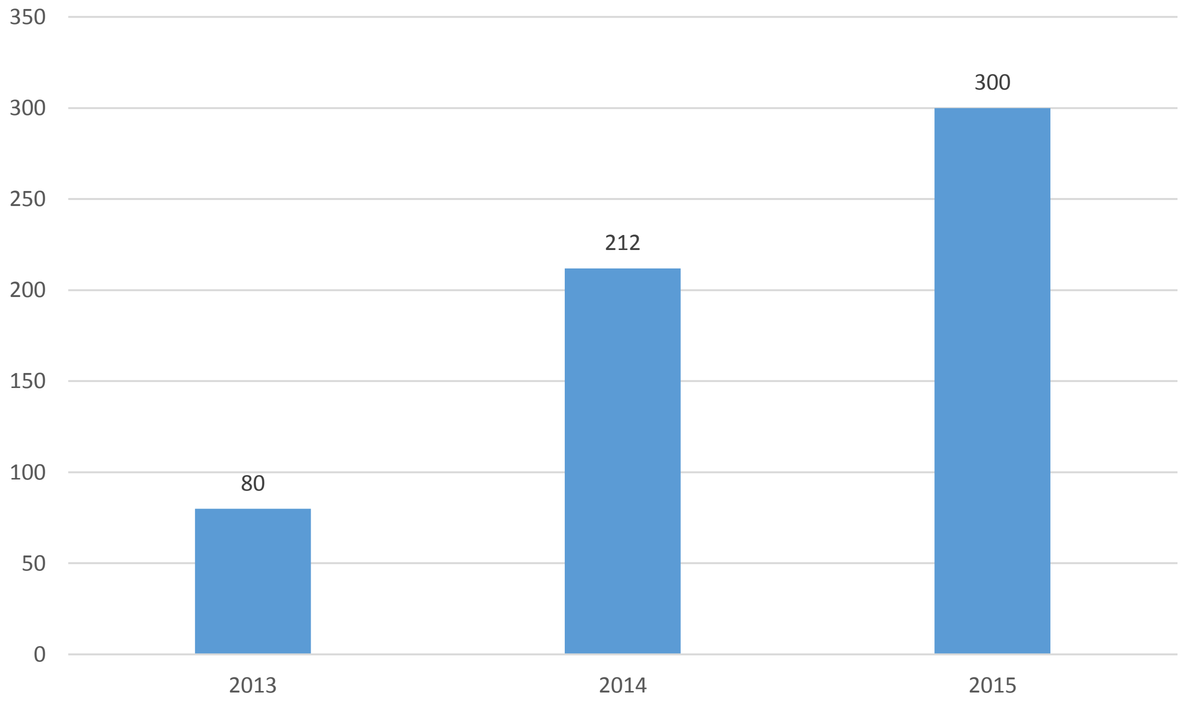
دبي الأولى
غيث المزينة
مدير خدمات جودة أمن المعلومات بالإنابة في هيئة تنظيم الاتصالات
دبي هذا الصباح

شرطة دبي DUBAI POLICE

الأمين al ameen

TRA هيئة تنظيم الاتصالات TELECOMMUNICATIONS REGULATORY AUTHORITY

Blackmail Numbers are growing



Source: Al Ameen Service

Causes for Cyber Blackmail

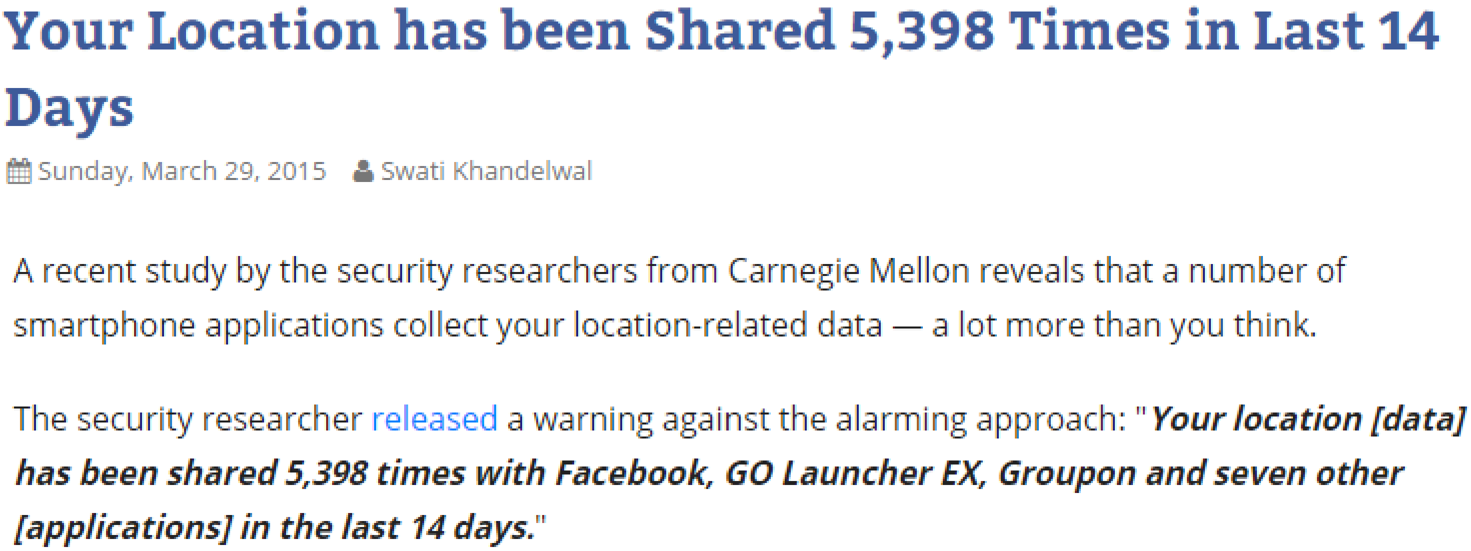
- Revealing private data
- Installing apps without reading the terms of use
- Insecure Practices

Revealing Private Data

- Attackers use personal data to choose their targets
  - i.e. Sharing the location with photos
- Anything you share on the Internet, will not be yours anymore
  - i.e. Saving Snapchat videos using third-party apps
- Don’t trust the other side, anything they say could be false
  - i.e. They could fake their identity

Not Reading the Terms of Use

- Some apps do things you might not have expected



Your Location has been Shared 5,398 Times in Last 14 Days

Sunday, March 29, 2015 Swati Khandelwal

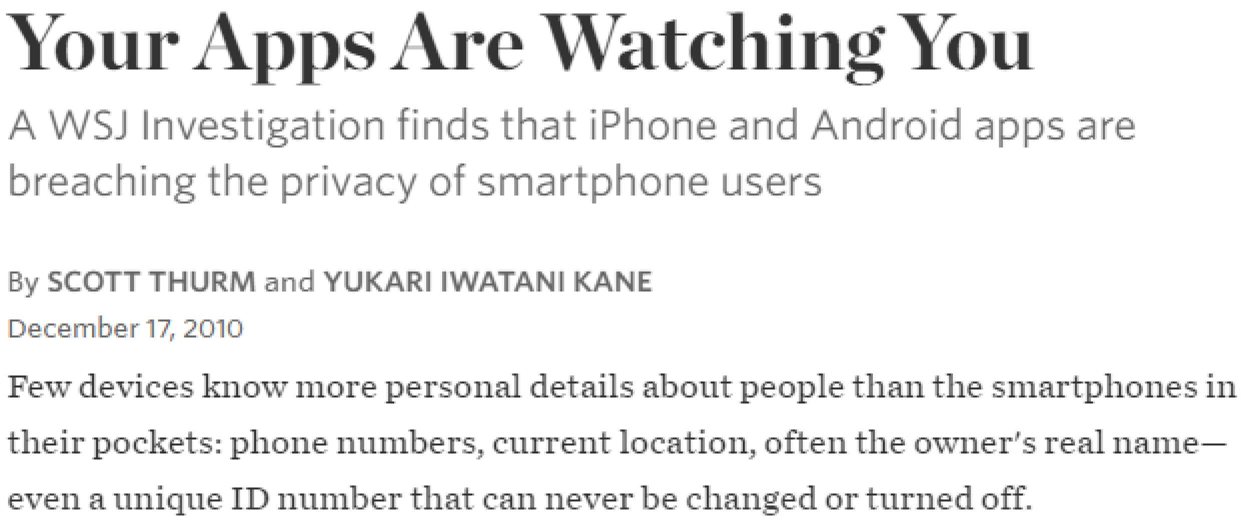
A recent study by the security researchers from Carnegie Mellon reveals that a number of smartphone applications collect your location-related data — a lot more than you think.

The security researcher released a warning against the alarming approach: "***Your location [data] has been shared 5,398 times with Facebook, GO Launcher EX, Groupon and seven other [applications] in the last 14 days.***"

http://thehackernews.com/2015/03/location-sharing-apps.html

Not Reading the Terms of Use

- Some app could share/sell your data with third-parties



Your Apps Are Watching You

A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users

By SCOTT THURM and YUKARI IWATANI KANE

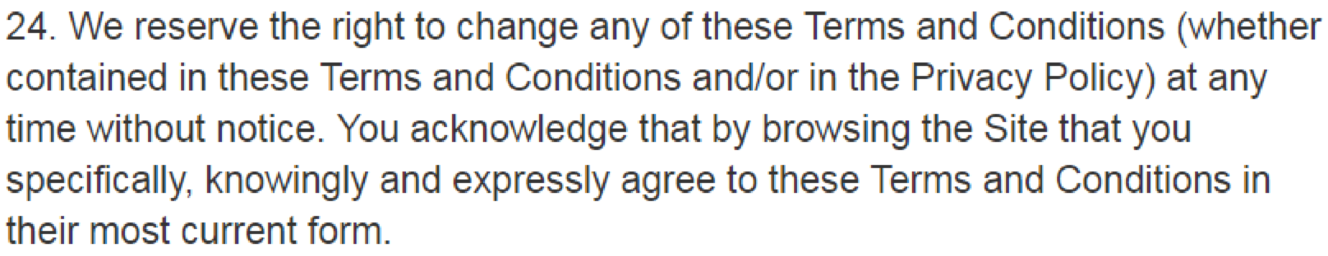
December 17, 2010

Few devices know more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner's real name—even a unique ID number that can never be changed or turned off.

http://www.wsj.com/articles/SB10001424052748704694004576020083703574602

Not Reading the Terms of Use

- Terms of Use could be changed without your knowledge
- You are considered to be agreeing to them
- An example:



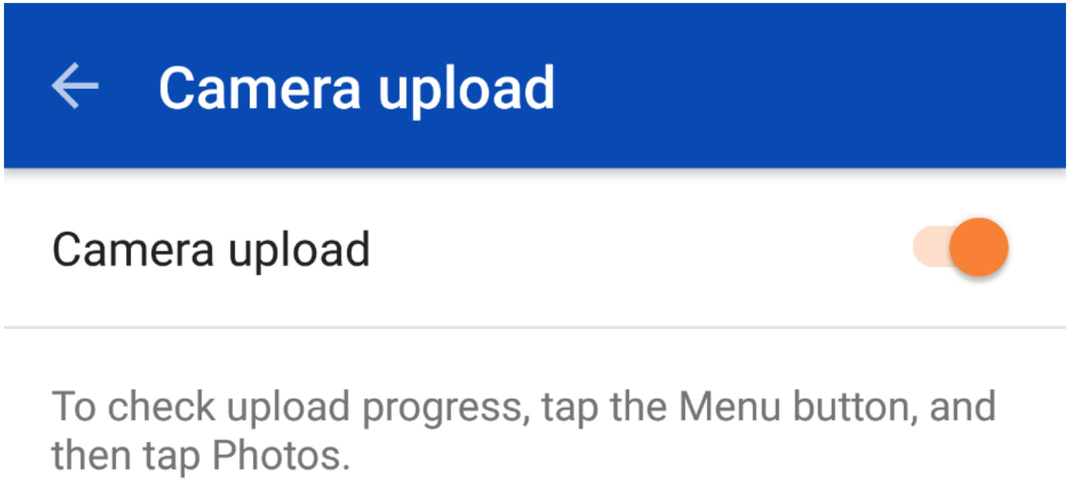
24. We reserve the right to change any of these Terms and Conditions (whether contained in these Terms and Conditions and/or in the Privacy Policy) at any time without notice. You acknowledge that by browsing the Site that you specifically, knowingly and expressly agree to these Terms and Conditions in their most current form.

Insecure Practices

- Easy passwords
  - Stealing personal data from accounts
- Recommendations
  - Minimum of 8 characters
  - A combination of letters, digits, and symbols
  - password => P@$$w0rd

Insecure Practices

- Some apps upload photos and videos from the gallery by default

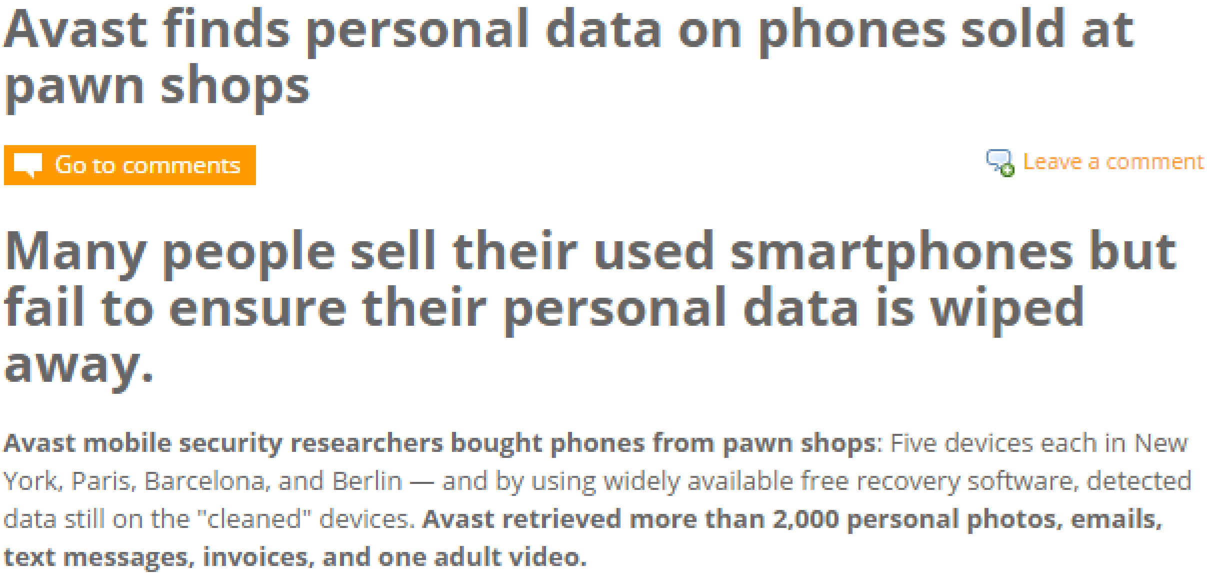


Camera upload ●

To check upload progress, tap the Menu button, and then tap Photos.

Insecure Practices

- Delete the data insecurely



Avast finds personal data on phones sold at pawn shops

Many people sell their used smartphones but fail to ensure their personal data is wiped away.

Avast mobile security researchers bought phones from pawn shops: Five devices each in New York, Paris, Barcelona, and Berlin — and by using widely available free recovery software, detected data still on the "cleaned" devices. **Avast retrieved more than 2,000 personal photos, emails, text messages, invoices, and one adult video.**

https://blog.avast.com/2016/02/24/avast-finds-personal-data-on-phones-sold-at-pawn-shops/

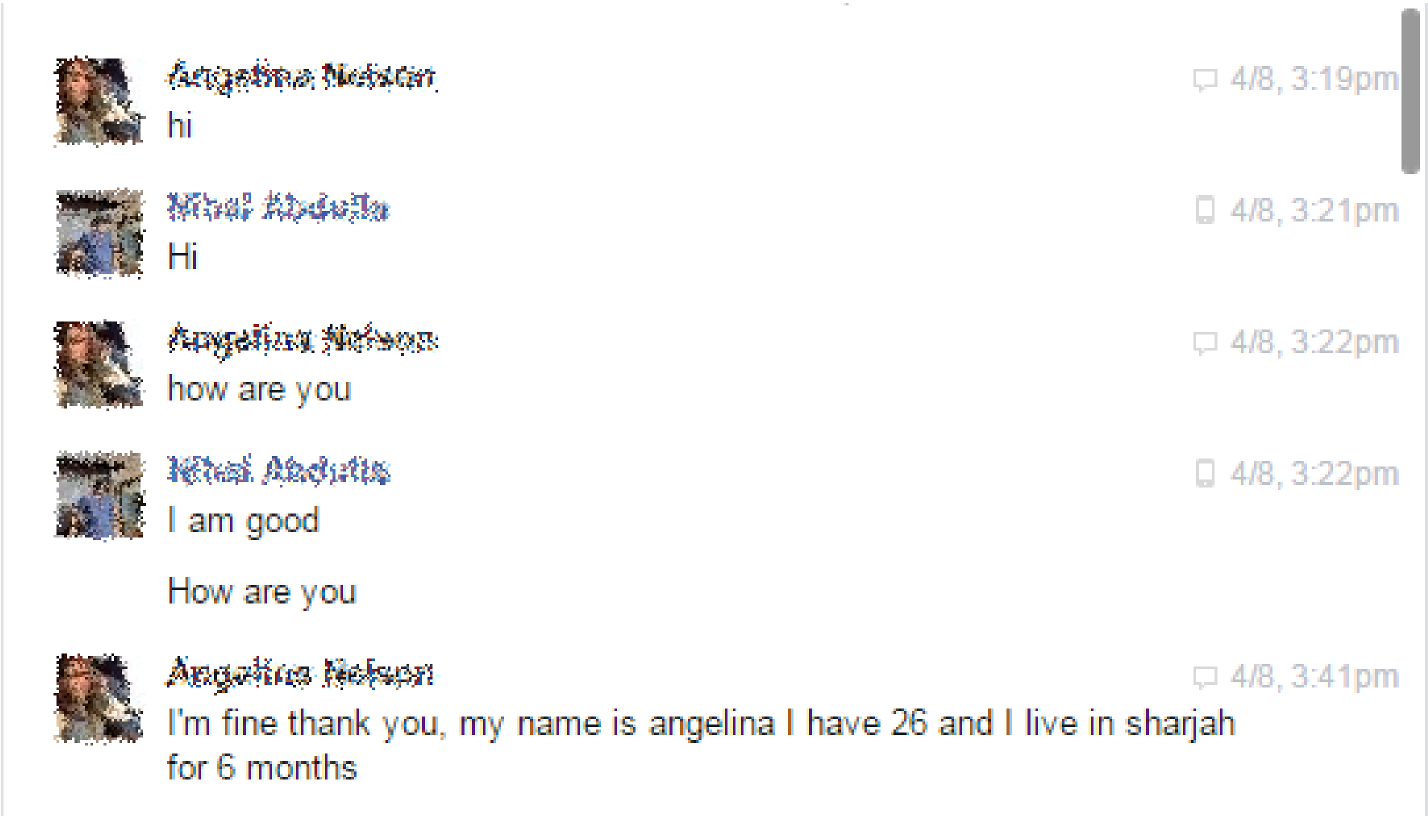
How the blackmailing is done

1. Gathering information about your interests and those who are close to you
2. Opening a direct communication with you
3. Building a close relationship and starting video calls
4. Opening a sexually explicit dialogue or filming sexual practices

How the blackmailing is done

5. Asking you to do the same, and record you while doing that (without your knowledge)
6. Disclosure of their real gender and identity
7. Blackmailing using the recorded material
8. Threatening to send the video to your close people, unless you pay money

Real Example



[redacted] 4/8, 3:19pm
hi

[redacted] 4/8, 3:21pm
Hi

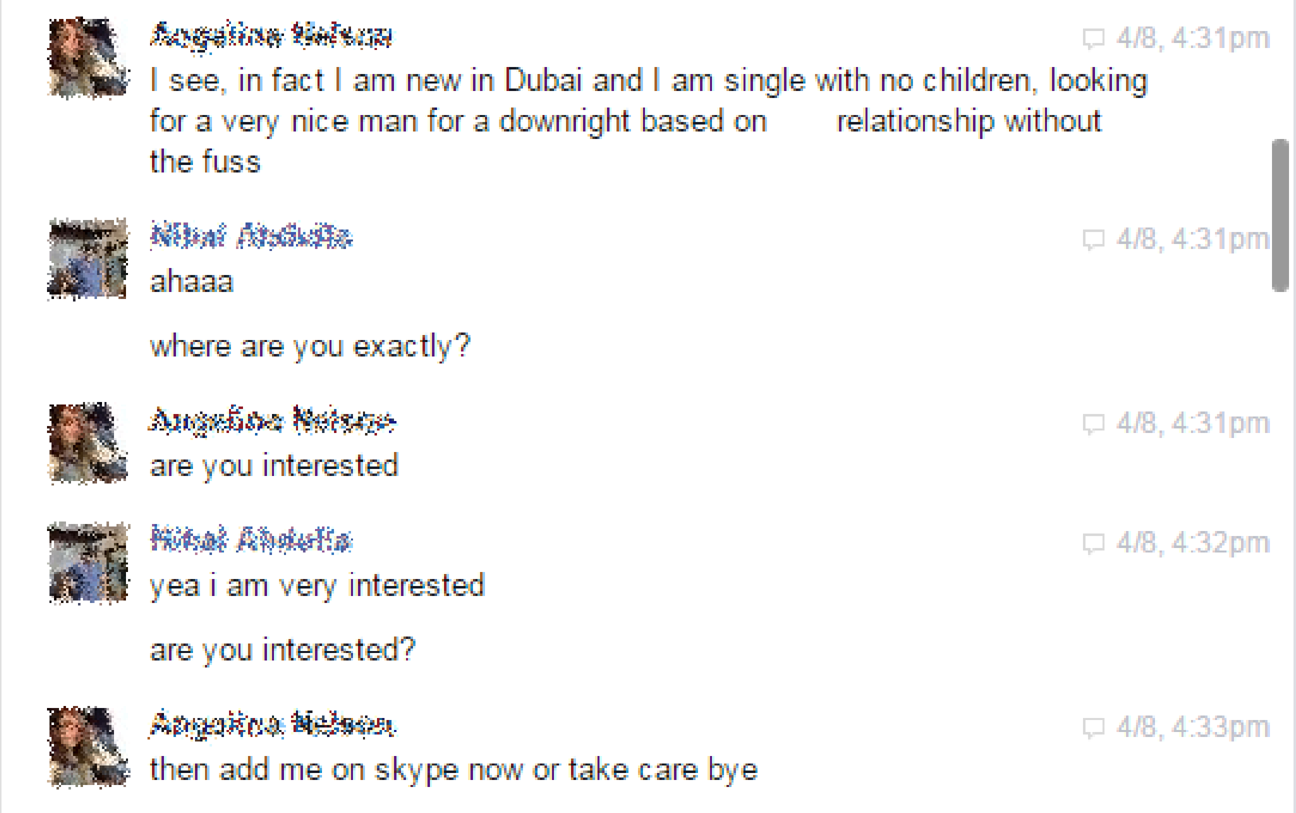
[redacted] 4/8, 3:22pm
how are you

[redacted] 4/8, 3:22pm
I am good

How are you

[redacted] 4/8, 3:41pm
I'm fine thank you, my name is angelina I have 26 and I live in sharjah for 6 months

Real Example



[redacted] 4/8, 4:31pm
I see, in fact I am new in Dubai and I am single with no children, looking for a very nice man for a downright based on relationship without the fuss

[redacted] 4/8, 4:31pm
ahaaa

where are you exactly?

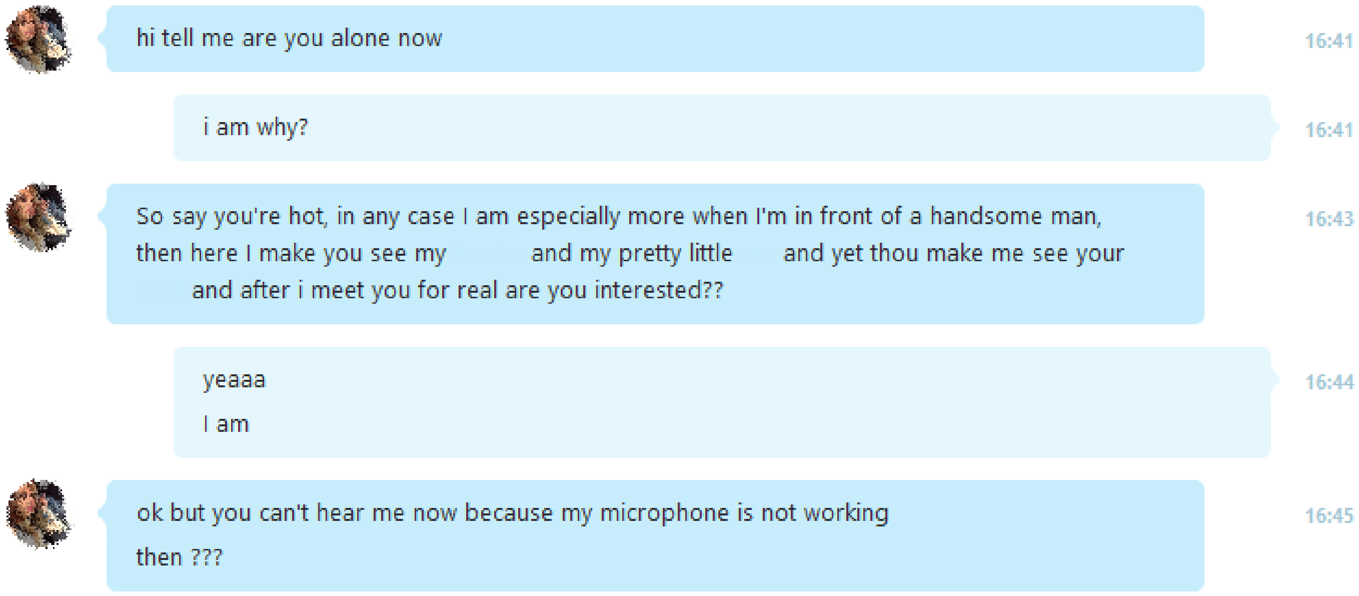
[redacted] 4/8, 4:31pm
are you interested

[redacted] 4/8, 4:32pm
yea i am very interested

are you interested?

[redacted] 4/8, 4:33pm
then add me on skype now or take care bye

Real Example



hi tell me are you alone now 16:41

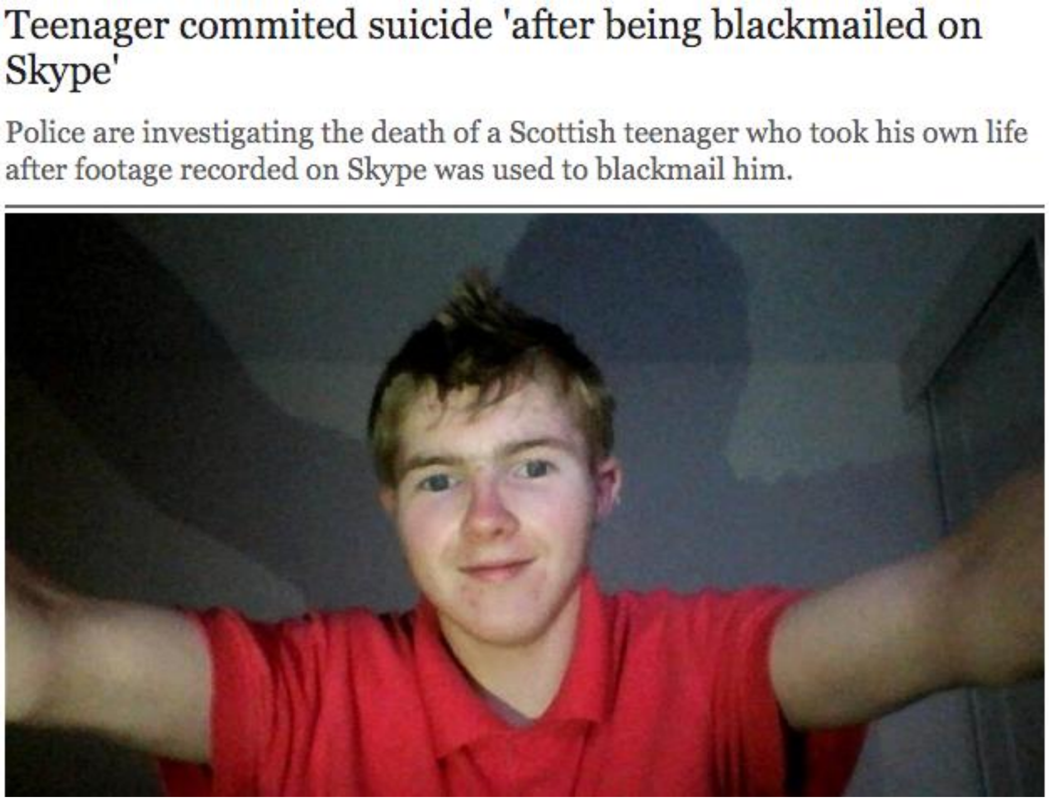
i am why? 16:41

So say you're hot, in any case I am especially more when I'm in front of a handsome man, then here I make you see my and my pretty little and yet thou make me see your and after i meet you for real are you interested?? 16:43

yeaaa
I am 16:44

ok but you can't hear me now because my microphone is not working
then ??? 16:45

Impact of blackmail



Teenager commited suicide 'after being blackmailed on Skype'

Police are investigating the death of a Scottish teenager who took his own life after footage recorded on Skype was used to blackmail him.

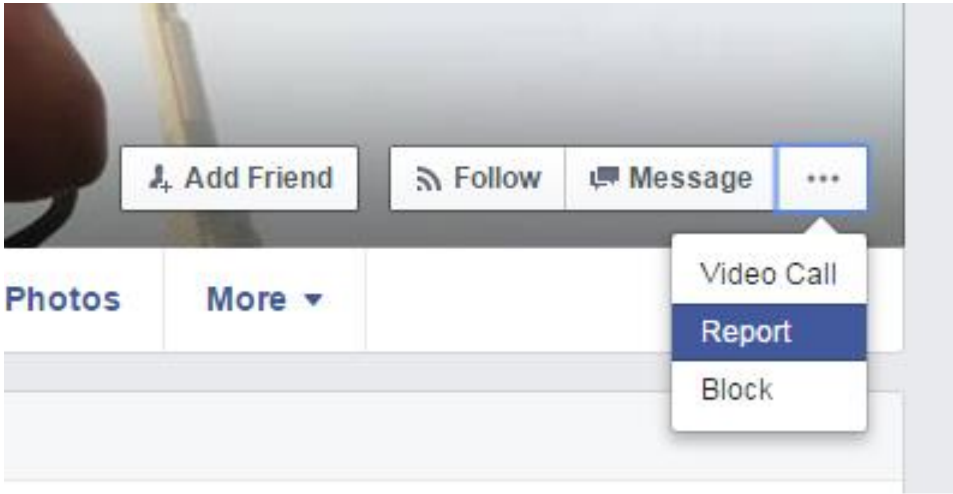
http://www.telegraph.co.uk/news/uknews/crime/10245809/Teenager-commited-suicide-after-being-blackmailed-on-Skype.html

If you fall a victim..

- Never send money under any direct threat
  - If you do so you will keep getting blackmailed.
- Report through police stations to provide a formal report
  - They will take the legal action for either national or international prosecution

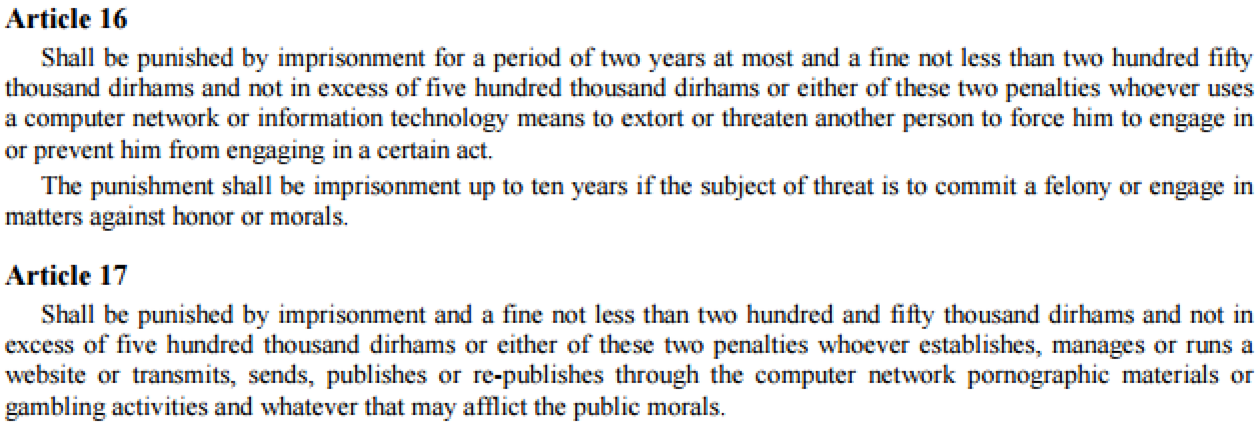
If you fall a victim..

- Report the attacker through the corresponding section at the social media website



If you fall a victim..

- Know the cyber crime laws in your country
- Example from UAE Cyber Crimes law



Article 16

Shall be punished by imprisonment for a period of two years at most and a fine not less than two hundred fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever uses a computer network or information technology means to extort or threaten another person to force him to engage in or prevent him from engaging in a certain act.

The punishment shall be imprisonment up to ten years if the subject of threat is to commit a felony or engage in matters against honor or morals.

Article 17

Shall be punished by imprisonment and a fine not less than two hundred and fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever establishes, manages or runs a website or transmits, sends, publishes or re-publishes through the computer network pornographic materials or gambling activities and whatever that may afflict the public morals.

To protect yourself..

- Read the terms and conditions of the apps before installing them
- Use a strong password and enable 2-factor authentication
- Never upload private photos on social networking accounts

To protect yourself..

- Don’t add strangers to your friends list
- Avoid dating websites and applications
  - They are often the starting point of enticing victims
- Remember that anything you share on the Internet, will not be yours anymore

To protect your children..

- Spend time and communicate more with your children
- Instruct the children on the dangers of the misuse of Internet and social media applications
- Limit the time of their usage of Internet
- Follow their accounts and try to understand their habits and activities on the social media

To protect your children..

- Enable parental control feature in their devices
- Use the safe mode feature in the apps they use
- Control the apps they install
- Educate them on the cyber security laws

Thank you