Understand the impact, before you share

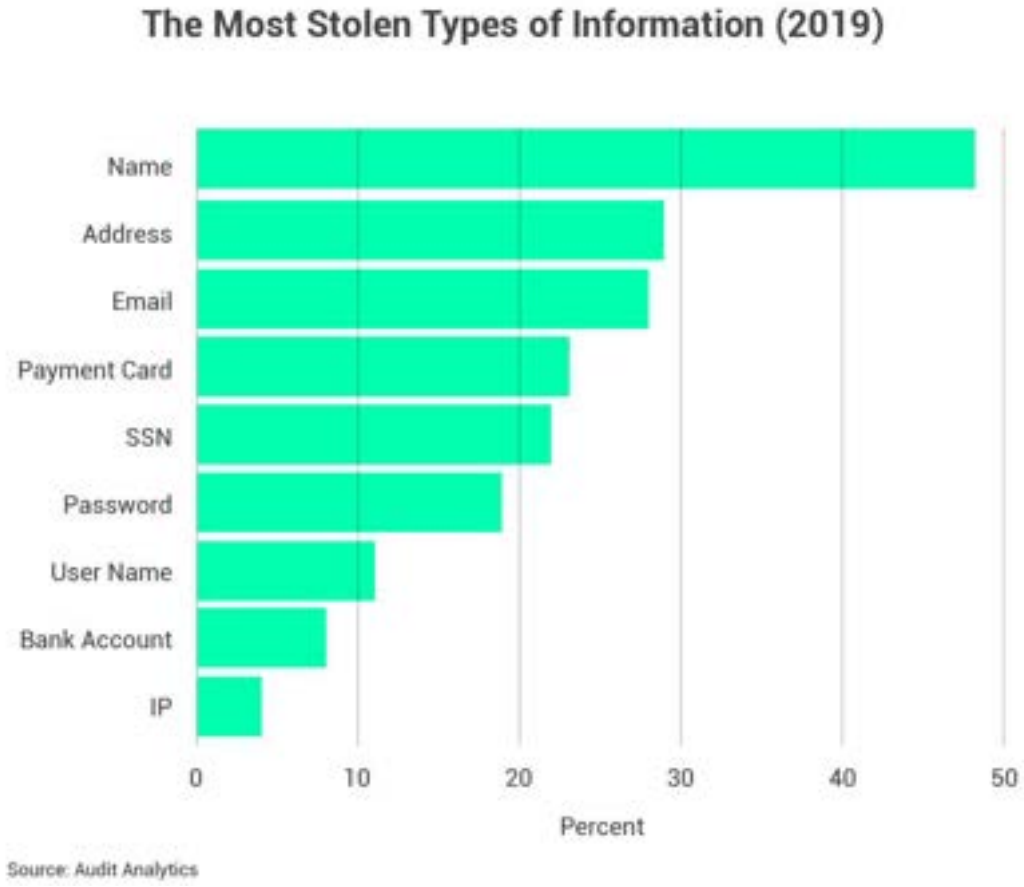
CHAN Chun Fai

Common sharing channels

- Social medias
  - Facebook
  - Instagram
  - Twitter
  - LinkedIn
- Blogs
- Online forums
- Dating apps
- Online games

Common personal information leaked

- Name
- Address
- Email
- Date of birth
- Phone numbers
- Photographs
- Locations
- Signature



Information engineering

- Name and address
  - Reveal your phone number, employment history, marriage status etc.
- Phone numbers
  - Reveal your addresses
- Photos
  - Reveal your locations and valuable items owned by you
  - Expose info of friends and social circles
- Hashtags
  - e.g. #ClassOf020 can reveal name of your school and graduation year
  - Age can then be deduced from graduation year

Common risks

- Theft of Identity
  - Depend on how much information is revealed
  - Fraudster can make use of the identity to
    - Enter unauthorized places
    - Open accounts at places like banks
    - Commit financial crimes
    - Guess your security questions on financial sites
    - Sell your personal information to third parties
    - Send phishing messages to you

Common risks

- Theft of property
  - Sharing photos on a trip tells criminals that you are out
  - By knowing your address, you are open to robbers

- Theft of passwords
  - Passwords can be deduced from you DOB, age, phone numbers etc.
  - Password hints can be guessed from your personal info

Real cases

A student in Bengaluru, Divya was a victim of identity theft recently. “Someone created a fake account of me on a dating site, using my pictures from Instagram. This led to a lot of misunderstanding and several people complained to me about receiving absurd messages from the account,” she says. The incident shocked her because her Instagram profile is private, where no outsider has easy access to her pictures.

“My account has always been private on Instagram, which is why I know it was someone I know and that is scary,” she adds.

Source: https://www.deccanherald.com/metrolife/metrolife-your-bond-with-bengaluru/identity-theft-a-big-problem-on-social-media-say-b-luru-youth-1050015.html

Real cases

One burglar in Orange County, California, targeted at least 33 women he saw in public and using GPS data embedded in photos posted to Facebook and Instagram to get to their homes in 2015. Once he had an address, court records showed, he stole more than $250,000 in electronics and jewelry along with his victims' underwear and bras.

Police across the country have been warning residents to be aware of what they post to social media. Police in Orange County cautioned women to check their settings on social media apps to disable location features after the rash or break-ins there.

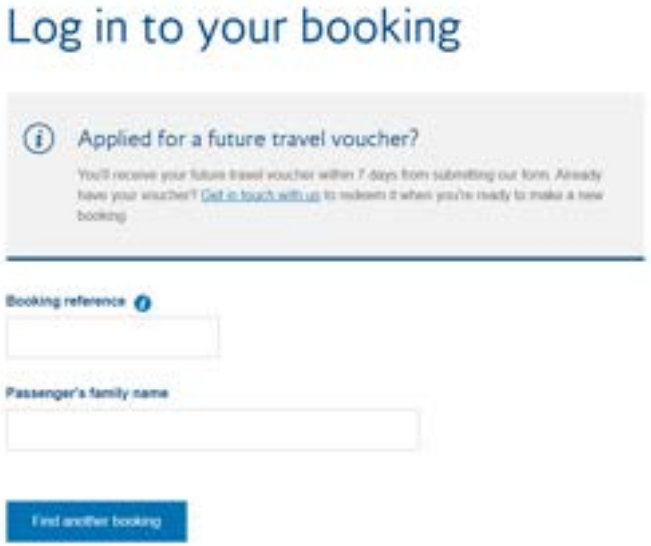
And in Prince William County, a suburban Virginia county outside Washington, police warned residents to avoid publicly posting photos of new items or checking in on location-based apps because of the risk of being targeted by burglars.

Medina said he would warn homeowners to avoid posting that they're going on vacation or posting about what they have inside their homes because they don't know whether a friend or follower could be a potential burglar.

"You don't want your neighbor to know because he could be a burglar," he said. "He's got seven days to take whatever he wants (if you announce that you're leaving on social media.)"

Source: https://www.nbcnewyork.com/news/local/investigations-i-team-social-media-use-survey-new-york-new-jersey/1329983/

Boarding pass sharing



M1LEOPOLD/EMR
EZQ7092 GVALHRBA

- Name
- Booking reference
- Time and location

→

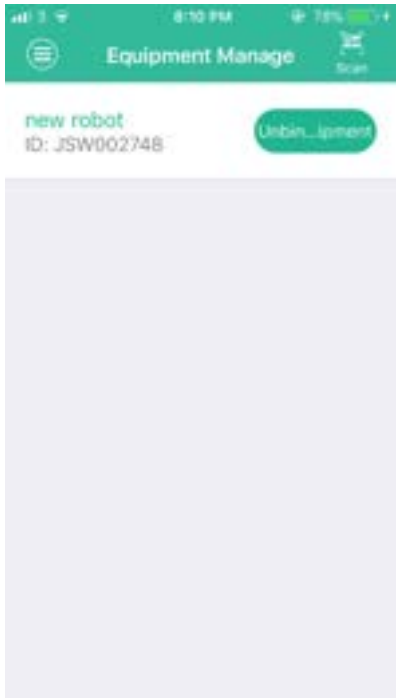
- Flyer account
- Last Name

→

- DOB
- Address
- Credit card

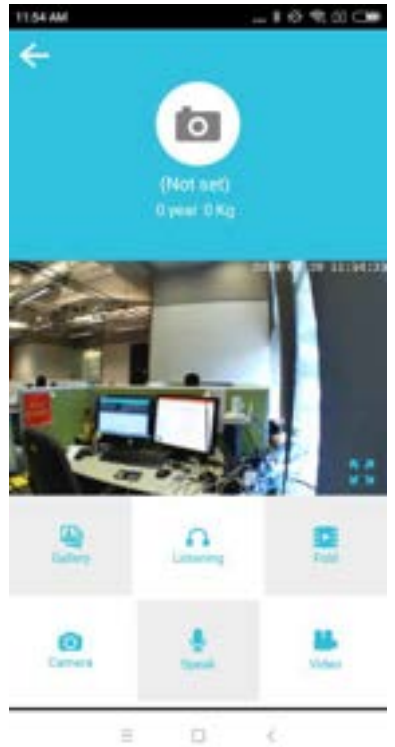
Sharing video about unboxing your new product

- Smart vacuum cleaner
  - How it works?
    - Register in vendor’s cloud
    - Bind the device by QR code
    - Login to cloud service and connect to the device



Sharing your Wifi

- Pet feeder
  - Now with “security camera”
  - Two way communications (listen + speak)
  - Regular feeding automatically
- Multiple vulnerabilities exists
  - Insecure web CGI
  - Backdoor available
  - Admin passwords stored in plain text!



Data leak from hacked websites

查询内容可以是QQ,账号ID,密码,邮箱账号,手机号,电话,身份证,姓名,微博uid,LOL用户名

搜索

◉ 综合查询 ○ 群关系 ○ 开房

账号	密码明文	密码MD5	密码MD5_2	salt	邮箱
An** L					an**********om
		5b**********0d			an**********om
		70**********36			an**********cn
	an***23				an**********cn

手机	身份证	地址
13*******16		汕头**********03

Things not to share

- Address and Phone Number
- Financial Data
- Private documents
- Travel Ticket/Boarding Pass
- Selfie while holding ID card
- Current location
- Digital identity
- Pictures of Credit Cards and Paychecks
- WIFI access
- Product QR and barcodes