WHAT SECURITY IS ABOUT IN GENERAL?

Security is about protection of assets

- D. Gollmann, Computer Security, Wiley

Prevention

- take measures that prevent your assets from being damaged (or stolen)

Detection

- take measures so that you can detect when, how, and by whom an asset has been damaged

Reaction

- take measures so that you can recover your assets

REAL WORLD EXAMPLE

Prevention

- locks at doors, window bars, secure the walls around the property, hire a guard

Detection

- missing items, burglar alarms,….

Reaction

- attack on burglar (not recommended ☺), call the police, replace stolen items, make an insurance claim

Buat yg belum bisa pasang CCTV


CAMOUFLAGE LEVEL: ANTI THEFT
VIA 1CAK.COM
MemeCenter.com
1CAK.COM/1262431

VIA 1CAK.COM


THE
NEIGHBORS
HAVE BETTER
STUFF


SECURITY
IS ON FULL ALERT

INTERNET SHOPPING EXAMPLE

Prevention

- encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don't send card number via Internet

Detection

- an unauthorized transaction appears on your credit card statement

Reaction

- complain, dispute, ask for a new card number, sue (if you can find of course ☺)
- Or, pay and forget (a glass of cold water) ☺


BNI
Kode Otentikasi sudah dikirim ke telepon seluler Anda
+xxxxxxxxxx01. Masukkan Kode Otentikasi untuk menyetujui transaksi ini sebelum waktu tenggat transaksi habis.
Waktu tenggat transaksi: 03 menit 30 detik
Nama Merchant : Merchant
Jumlah Transaksi : IDR 10.000,00
Tanggal Transaksi : Sel 12 Mei 2020 09:45:27 GMT +0700
No. BNI : xxxx xxxx xxxx 0003
Kode Otentikasi :
Batal
Kirim Ulang Kode Otentikasi
OK
Jangan berikan Kode Otentikasi ini kepada orang lain.
Hubungi BNI Call 1500046 apabila transaksi Anda bermasalah.
3

INFORMATION SECURITY IN PAST & PRESENT

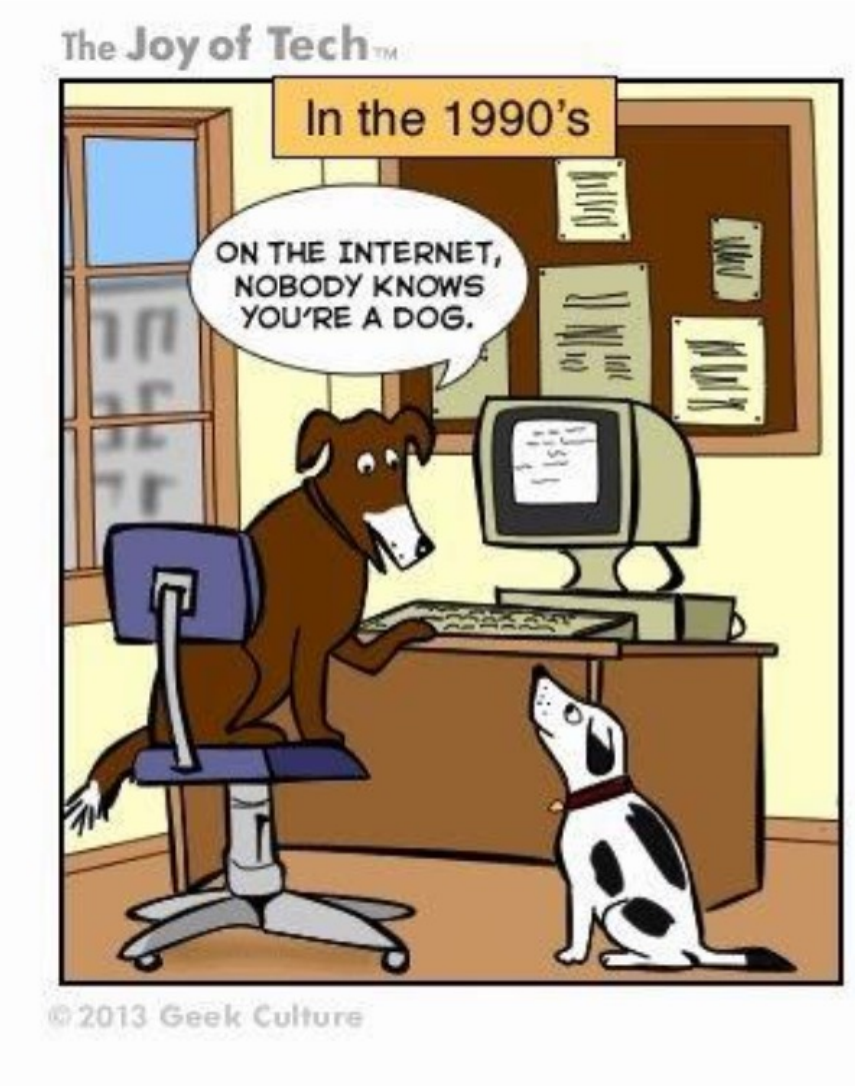
Traditional Information Security

- keep the cabinets locked
- put them in a secure room
- human guards
- electronic surveillance systems
- in general: physical and administrative mechanisms

Modern World

- Data are in computers
- Computers are interconnected

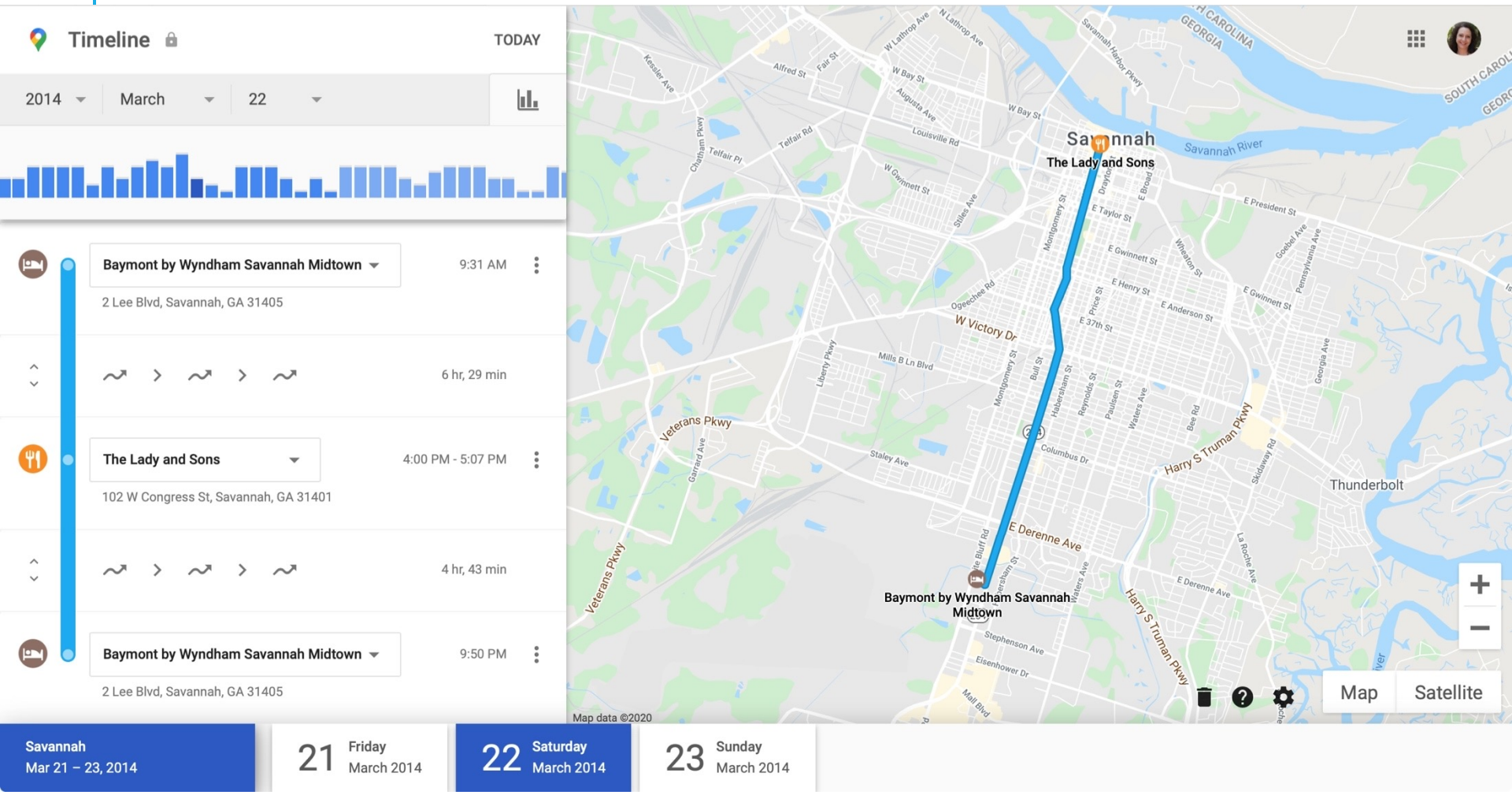
Computer and Network/Cyber Security



Our problem old days

Our problem today!

TIMELINE MAPS WAYBACK MACHINE


Timeline
TODAY
2014
March
22
Baymont by Wyndham Savannah Midtown
9:31 AM
2 Lee Blvd, Savannah, GA 31405
6 hr, 29 min
The Lady and Sons
4:00 PM - 5:07 PM
102 W Congress St, Savannah, GA 31401
4 hr, 43 min
Baymont by Wyndham Savannah Midtown
9:50 PM
2 Lee Blvd, Savannah, GA 31405
Savannah
The Lady and Sons
Savannah River
Baymont by Wyndham Savannah Midtown
Thunderbolt
W Victory Dr
E Derenne Ave
Veterans Pkwy
Harry S Truman Pkwy
Map data ©2020
Map
Satellite
Savannah
Mar 21 – 23, 2014
21 Friday March 2014
22 Saturday March 2014
23 Sunday March 2014

web.archive.org/web/20020925214109/http://www.unklab.ac.id/

INTERNET ARCHIVE WayBackMachine

http://www.unklab.ac.id/ Go

842 captures
25 Sep 2002 - 10 Jun 2023

AUG SEP 25 MAR
2001 2002 2003

Thursday, September 26, 2002

UNIVERSITAS KLABAT

STUDENT UNIVERSITY RESEARCH CONTACT US

Home | History | Academic | Admission | Administration | Academic Calendar | News | Event | Alumni | Photo Archive

+ student LOGIN

STUDENT ID

PASSWORD

login

forget password

+ unklab NEWS

Mahasiswa Tidak Harus Tinggal Di Asrama

Mulai semester I 2002/2003 mahasiswa yang tinggal bersama orangtua kandung di sekitar Manado, Bitung dan Tondano tidak harus masuk asrama. Ketentuan baru ini baru ujicoba mulai semester 1 2002/2003 ...

click here for more

+ campus EVENTS

17 - 08 - 2002
Lomba tujuh belasan dalam lingkungan kampus

20 - 09 - 2002
Malam kesenian oleh Unklab Choir

+ academic CALENDER

17-18 August 2002
Ekstra Weekend

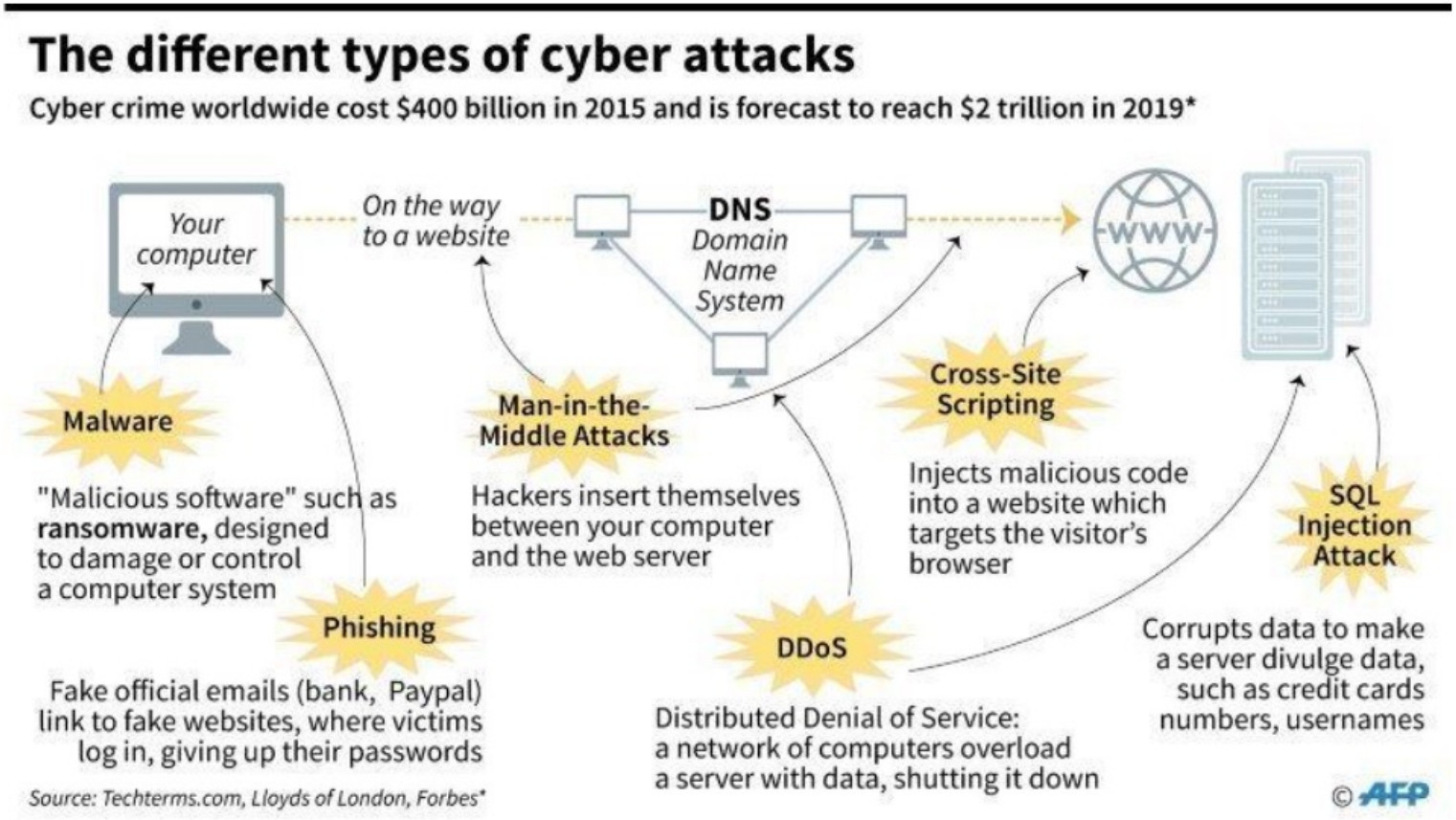
9-14 September 2002
Health Week

4-6 October 2002
Weekend Kelas Jumat

click here for more

Airmadidi, Manado 95371 - SULUT - INDONESIA
Telp. : (+62) 431 891035, 891041-42
Fax. : (+62) 431 891036
email : klabat@klabat.ac.id

Cyber Attacks Today



What is cyber security?

- **Cyber security** : perlindungan terhadap sistem informasi (hardware, software dan infrastruktur), data yang ada di dalamnya, dan layanan yang disediakan, dari penyalahgunaan akses yang tidak sah. [UK National Cyber Security Strategy]

A NOTE ON SECURITY TERMINOLOGY

No single and consistent terminology in the literature!

Be careful not to confuse while reading papers and books

Why need cyber security?

- Sistem bisa gagal karena berbagai alasan
- Sistem yang handal, dapat mengurangi kegagalan yang tidak disengaja
- Usabilitas sistem, dapat mengurangi kesalahan pengoperasian oleh pengguna
- **Keamanan** → mengurangi kegagalan yang disengaja yang dibuat oleh pihak-pihak yang 'cerdas'

Go to **www.menti.com** and use the code **3524 1197**

Apa akar masalah cyber security?

Mentimet

What drives attackers?

- Permusuhan
- Uang
- Ketenaran, kedengkian, keingintahuan
- Politik, teror, balas dendam, dll.
- “The lulz"

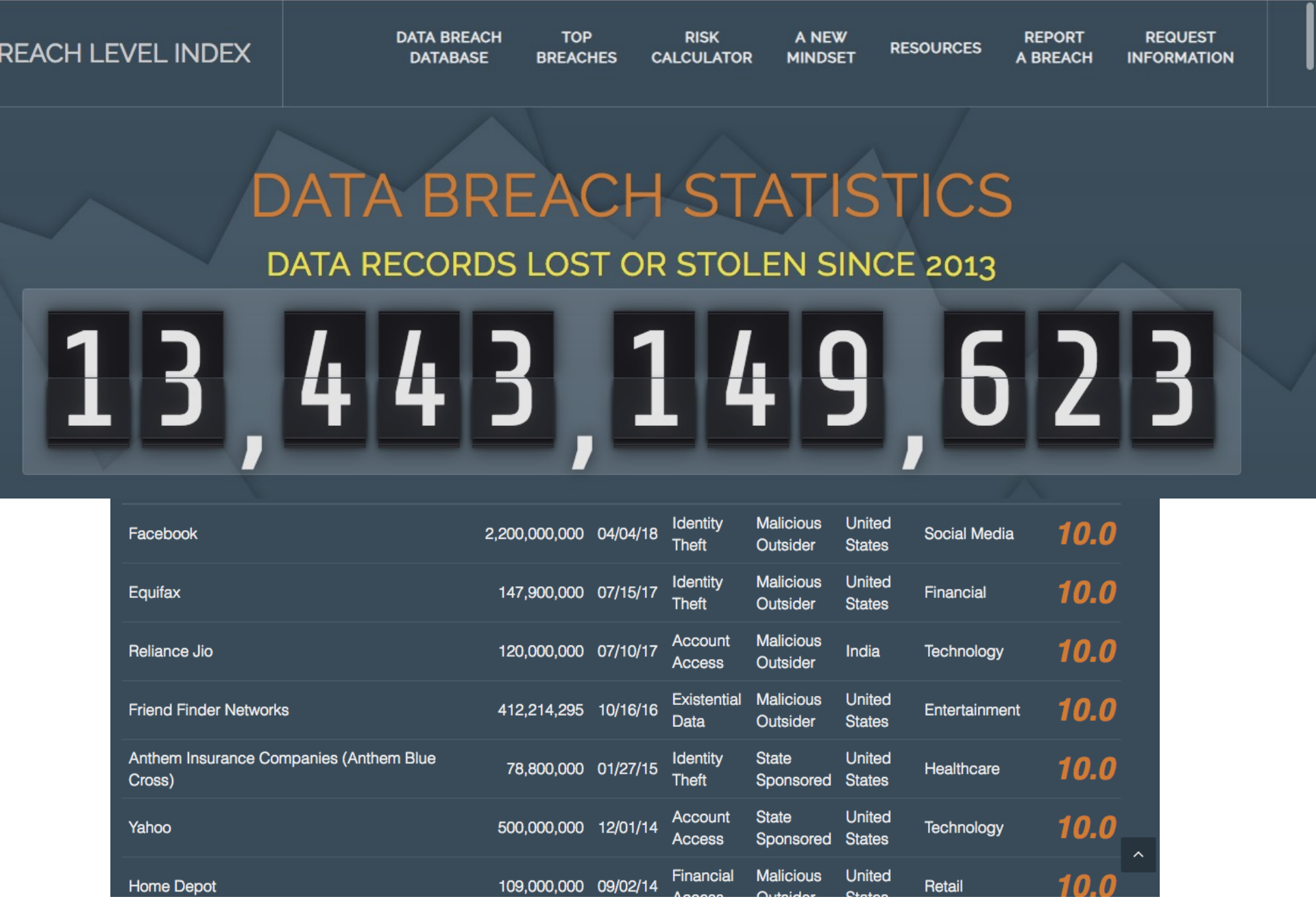
Go to **www.menti.com** and use the code **3524 1197**

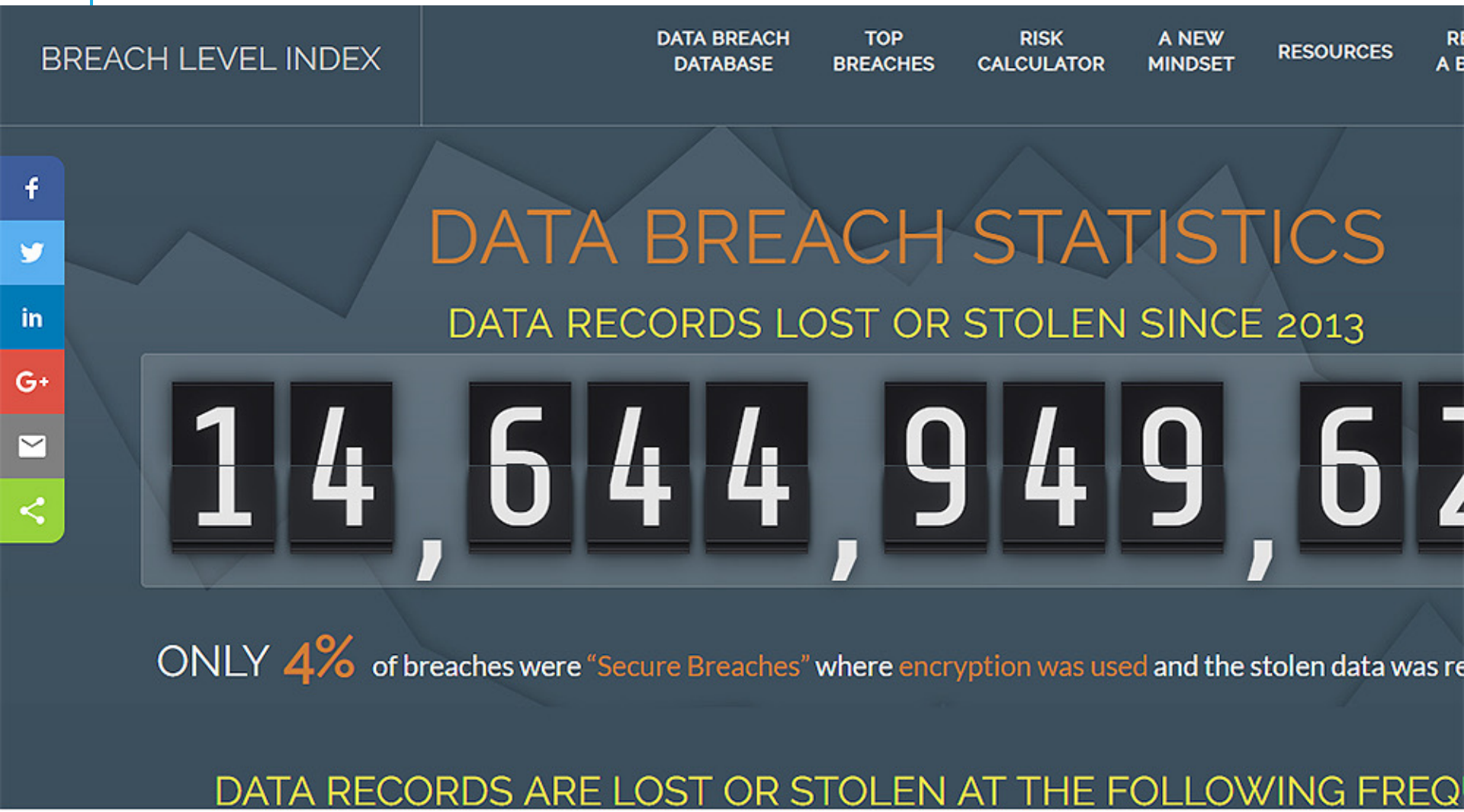
What drives attackers?

Mentimeter

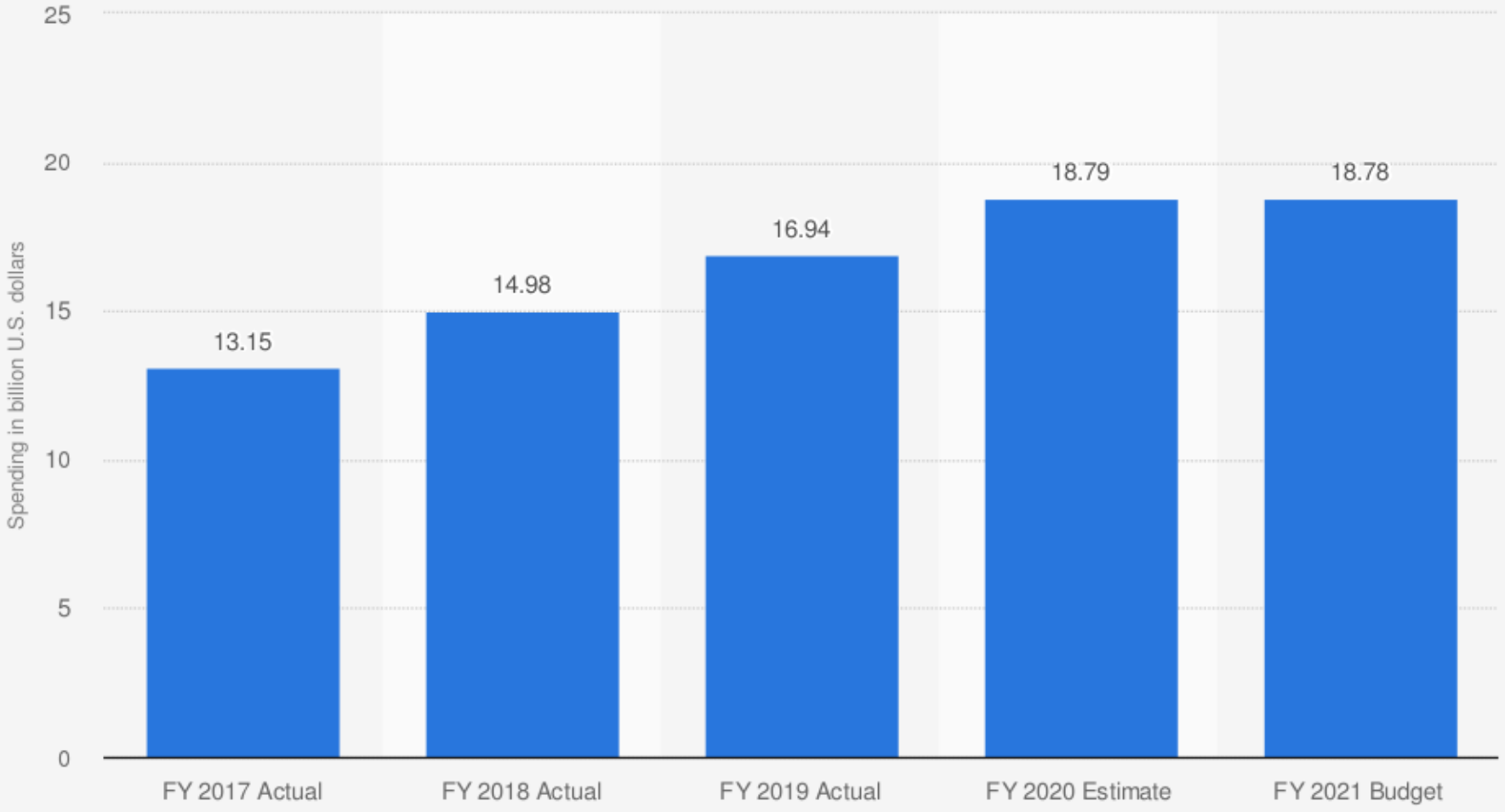
Primary Motivation? Money!

- Denial of service, extortion
- Ransomware
- Ad injection
- Pencurian uang (banking fraud, Bitcoin)
- Pencurian credit card (mall, restaurant, cafe)


REACH LEVEL INDEX
DATA BREACH DATABASE
TOP BREACHES
RISK CALCULATOR
A NEW MINDSET
RESOURCES
REPORT A BREACH
REQUEST INFORMATION
DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013
13,443,149,623
Facebook 2,200,000,000 04/04/18 Identity Theft Malicious Outsider United States Social Media 10.0
Equifax 147,900,000 07/15/17 Identity Theft Malicious Outsider United States Financial 10.0
Reliance Jio 120,000,000 07/10/17 Account Access Malicious Outsider India Technology 10.0
Friend Finder Networks 412,214,295 10/16/16 Existential Data Malicious Outsider United States Entertainment 10.0
Anthem Insurance Companies (Anthem Blue Cross) 78,800,000 01/27/15 Identity Theft State Sponsored United States Healthcare 10.0
Yahoo 500,000,000 12/01/14 Account Access State Sponsored United States Technology 10.0
Home Depot 109,000,000 09/02/14 Financial Malicious United Retail 10.0


BREACH LEVEL INDEX
DATA BREACH DATABASE
TOP BREACHES
RISK CALCULATOR
A NEW MINDSET
RESOURCES
DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013
14,644,949,6
ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was re
DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQ

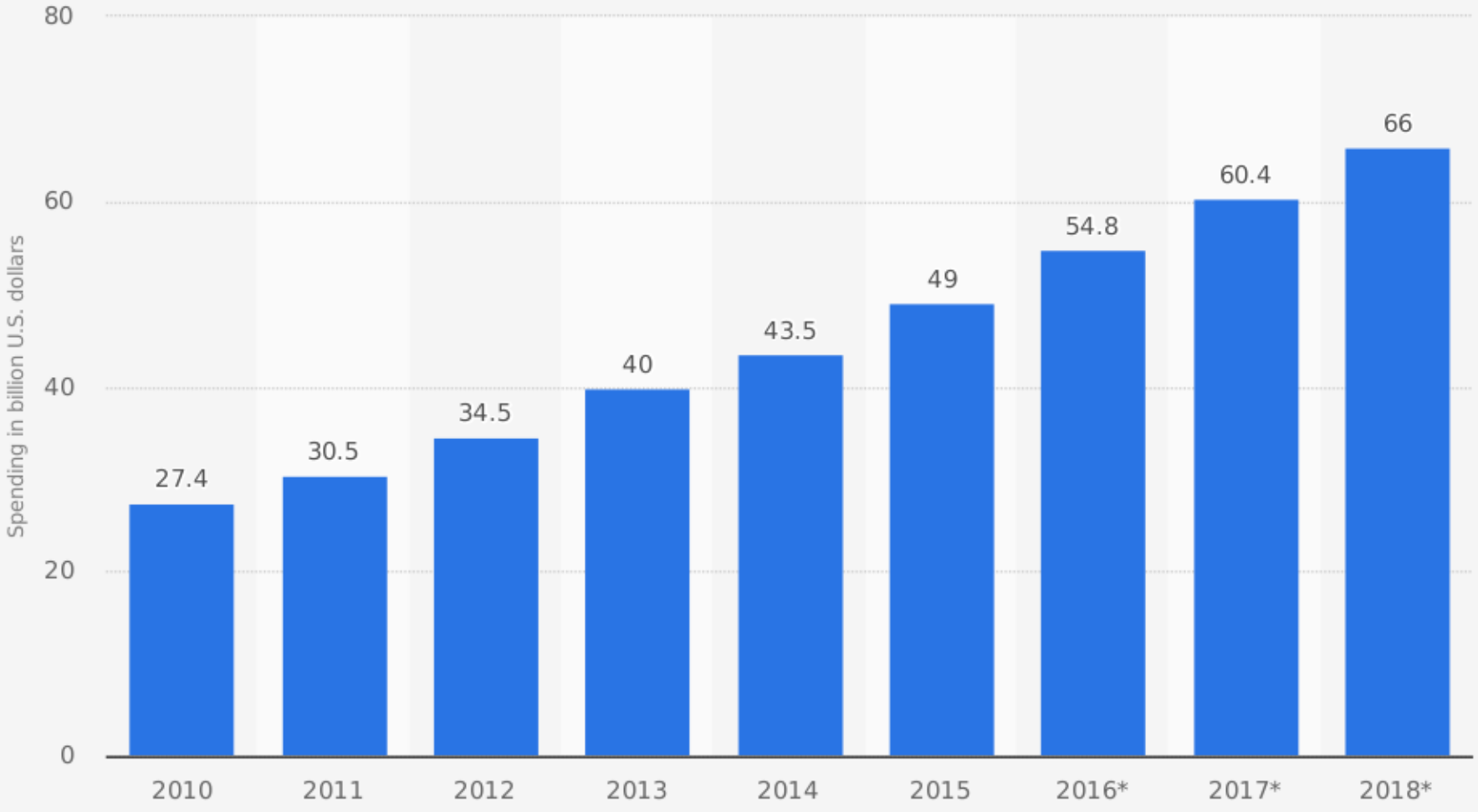
Proposed budget of the U.S. government for cyber security in FY 2017 to 2021 (in billion U.S. dollars)



Sources
US Congressional Budget Office; US Office of Management and Budget

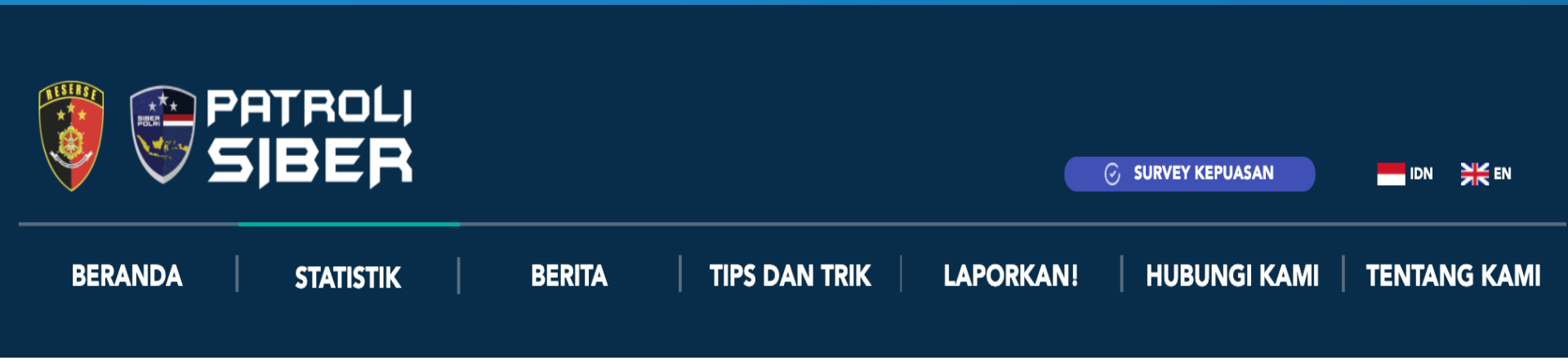
Additional Information:
United States; FY 2017 to FY 2019; CFO Act and non-CFO Act agencies

Spending on cybersecurity in the United States from 2010 to 2018 (in billion U.S. dollars)



Source
TIA

Additional Information:
United States; TIA; 2010 to 2015



Laporan Masyarakat melalui portal Patrolisiber

22.691

Total Aduan

5,05T

Total Kerugian

Filter Laporan

Jun 2016 - Jun 2021

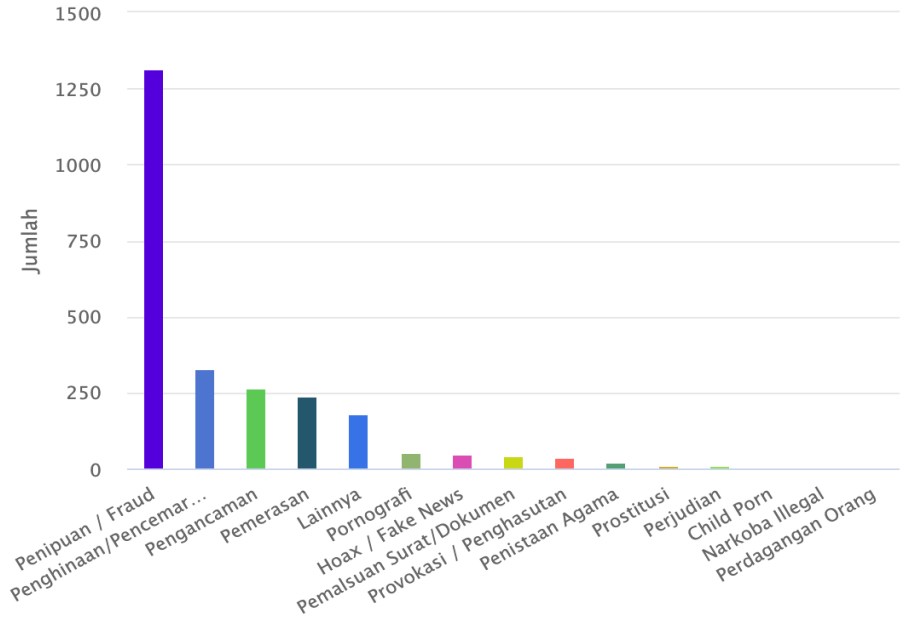
Sumber: https://patrolisiber.id/statistic

PATROLI SIBER

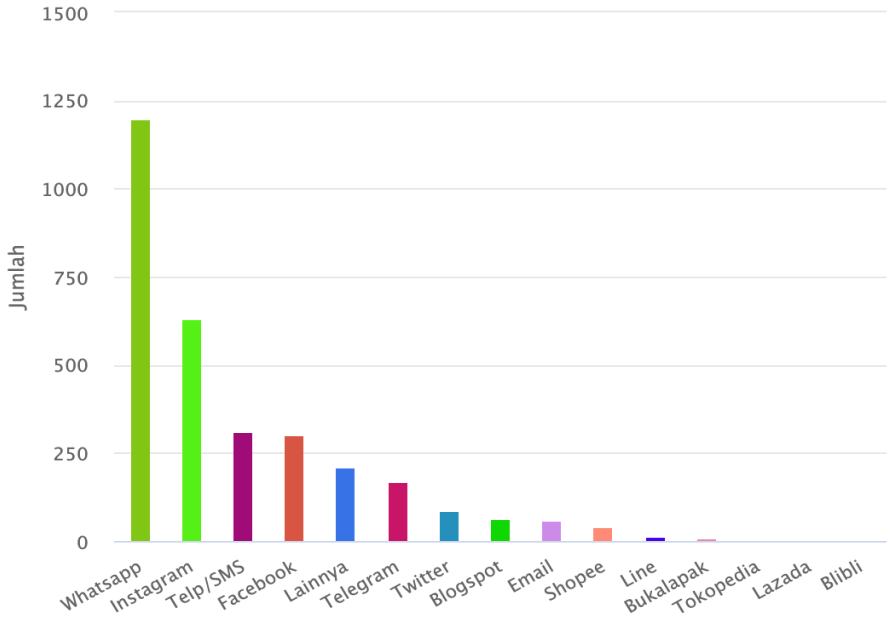
SURVEY KEPUASAN | IDN | EN

BERANDA | STATISTIK | BERITA | TIPS DAN TRIK | LAPORKAN! | HUBUNGI KAMI | TENTANG KAMI

Total Konten Negatif

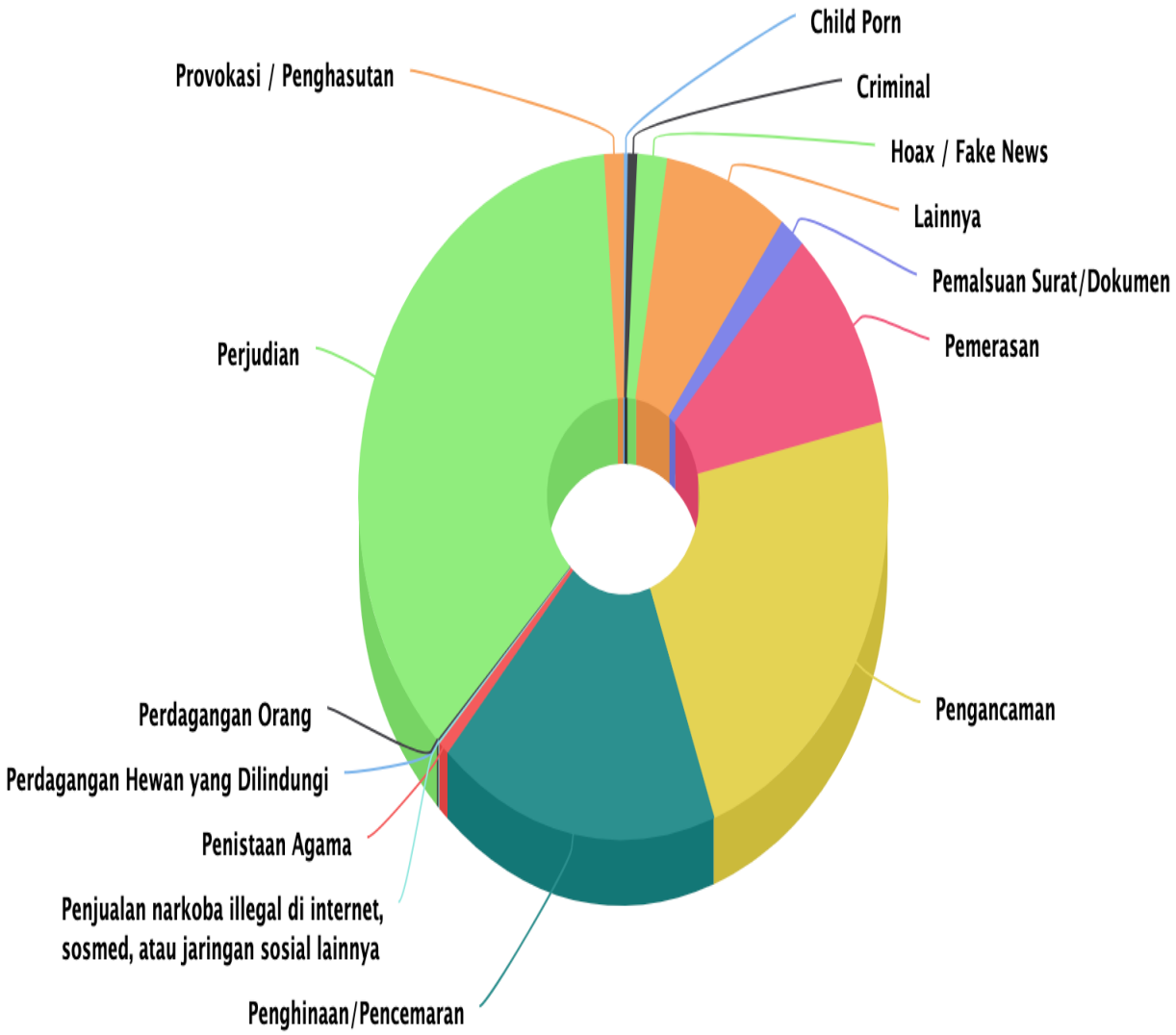


Total Platform Terlapor



Sumber: https://patrolisiber.id/statistic

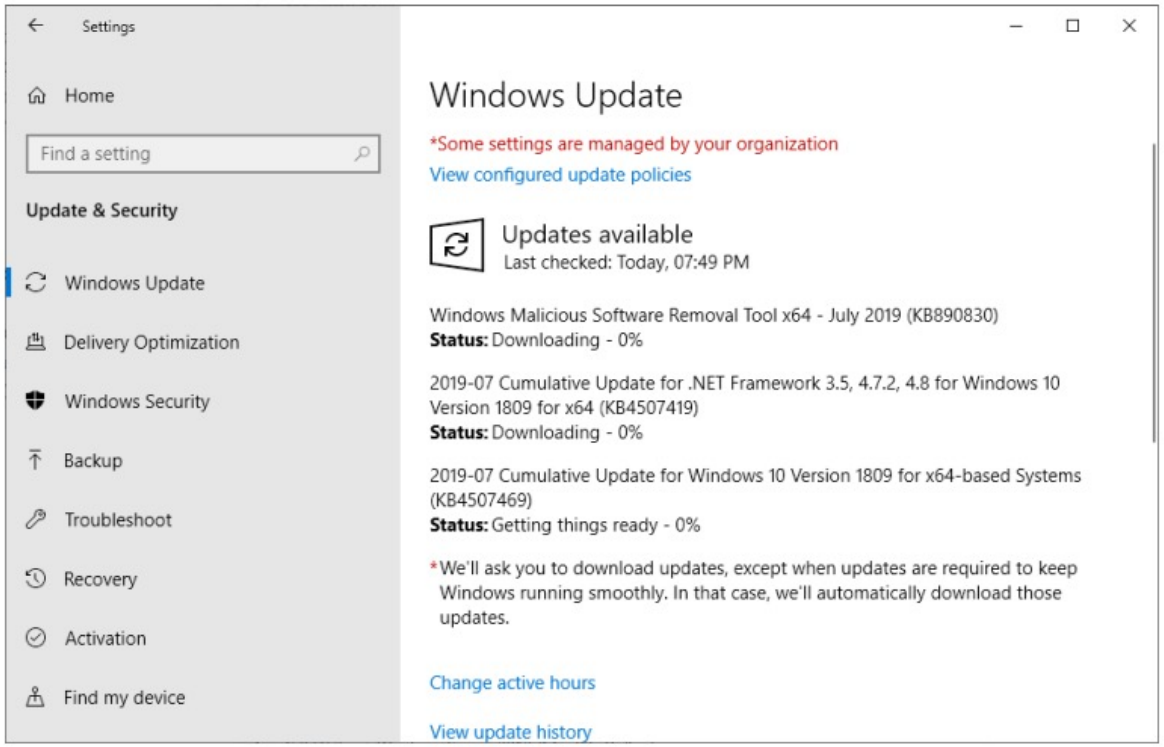
Sumber: https://patrolisiber.id/statistic

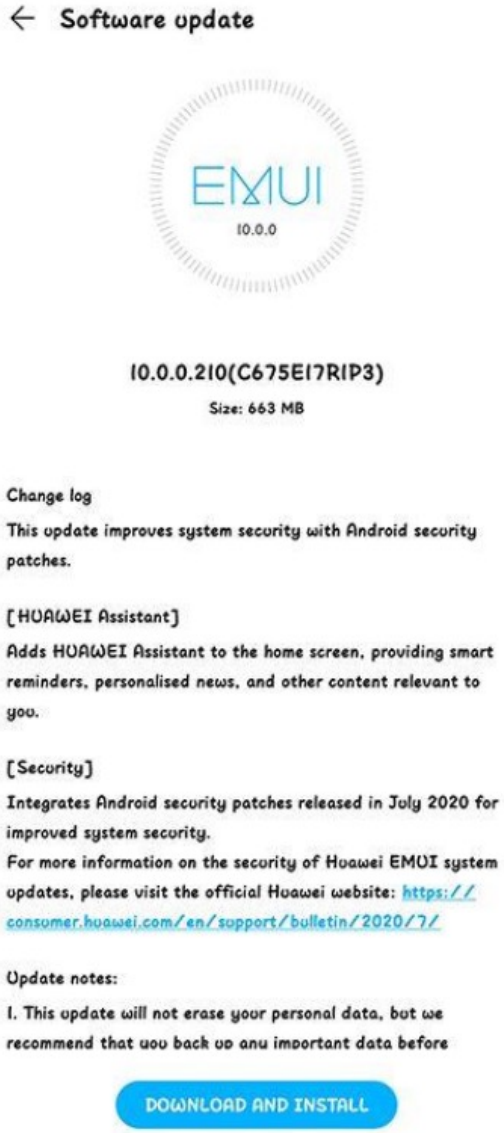

Child Porn
Criminal
Hoax / Fake News
Lainnya
Pemalsuan Surat/Dokumen
Pemerasan
Pengancaman
Penghinaan/Pencemaran
Penjualan narkoba illegal di internet, sosmed, atau jaringan sosial lainnya
Penistaan Agama
Perdagangan Hewan yang Dilindungi
Perdagangan Orang
Perjudian
Provokasi / Penghasutan

Why security failed?

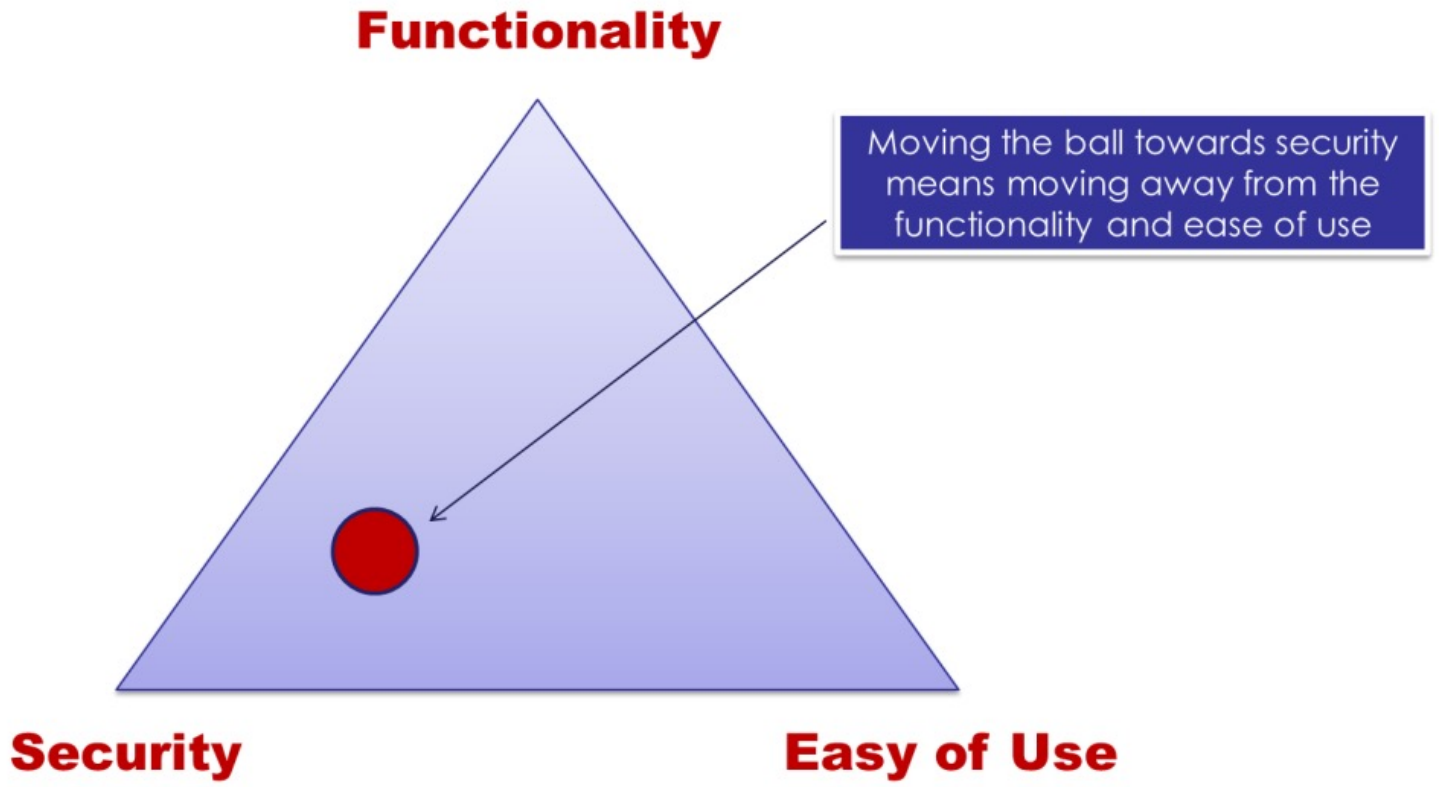
- Terrible software
- Bad network design
- Poor authentication
- Humans
- Bad policy

Terrible Software





Place the Red Dot



Most of the first computer applications had no or at best, very little, security. This lack of security continued for a number of years until the importance of data was truly realized. Until then, computer data was considered useful, but not something that needed to be protected. When computer applications were developed to handle financial and personal data, the real need for security was felt like never before. People realized that the data on computers is an extremely important aspect of modern life, and various areas in security began to gain importance.

The Internet is used globally, and there were many examples of what could happen if there was insufficient security built into the applications developed for the Internet. Figure 1.1 shows such an example of what can happen when you use your credit card for making purchases over the Internet. From the user's computer, the user's details, such as the user id, order details, such as the order id and item id, and payment details, such as the credit card information, travel across the Internet to the merchant's server. The merchant's server stores these details in its database.

There are various security holes in this process. First, an intruder can capture the credit card details as they travel from the client to the server. If we somehow protect this transit from an intruder's attack, it still does not solve our problem. Once the merchant receives the credit card details and validates them to process the order and obtain payments, the merchant stores the credit card details in its database. An attacker can simply access this database and gain access to all the credit a card numbers stored therein! One Russian attacker (called Maxim) managed to hack a merchant's Internet site and obtain 300,000 credit card numbers from its database. He then attempted extortion by demanding protection money ($100,000) from the merchant. The merchant refused to oblige. Following this, the attacker published about 25,000 of the credit card numbers on the Internet. Some banks reissued all the credit cards at a cost of $20 per card, and others warned their customers about unusual entries in their statements.

SELLING Tokopedia 91 million users for sale

by whysodank - Yesterday at 08:40 PM

whysodank

V.I.P User

VIP

Posts	6
Threads	3
Joined	Apr 2020
Reputation	20

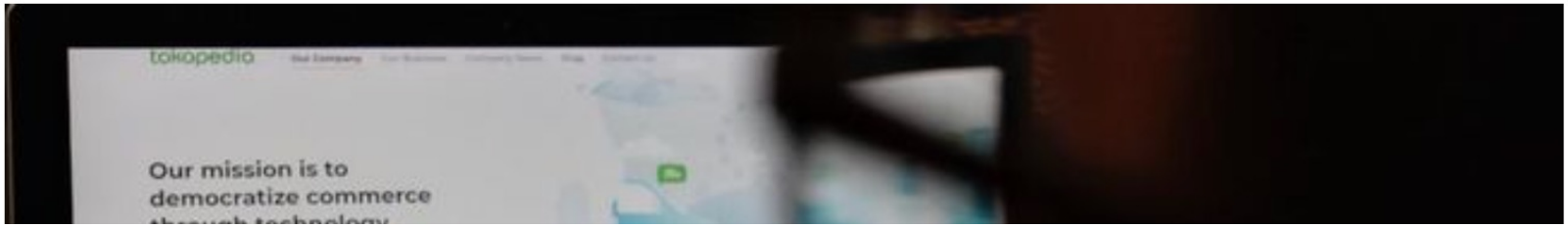
Yesterday at 08:40 PM This post was last modified: 10 hours ago by whysodank. Edited 1 time in total.

Hello.So the full tokopedia is for sale on empire market:
http://gshgz5zl2blfqbltnlbzpxn6icu3iue74...49/1008904
Feel free to PM me here too.
I already post some samples:
https://raidforums.com/Thread-UPDATE-Exc...lion-users

Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual

CNN Indonesia

Minggu, 03 Mei 2020 15:41 WIB



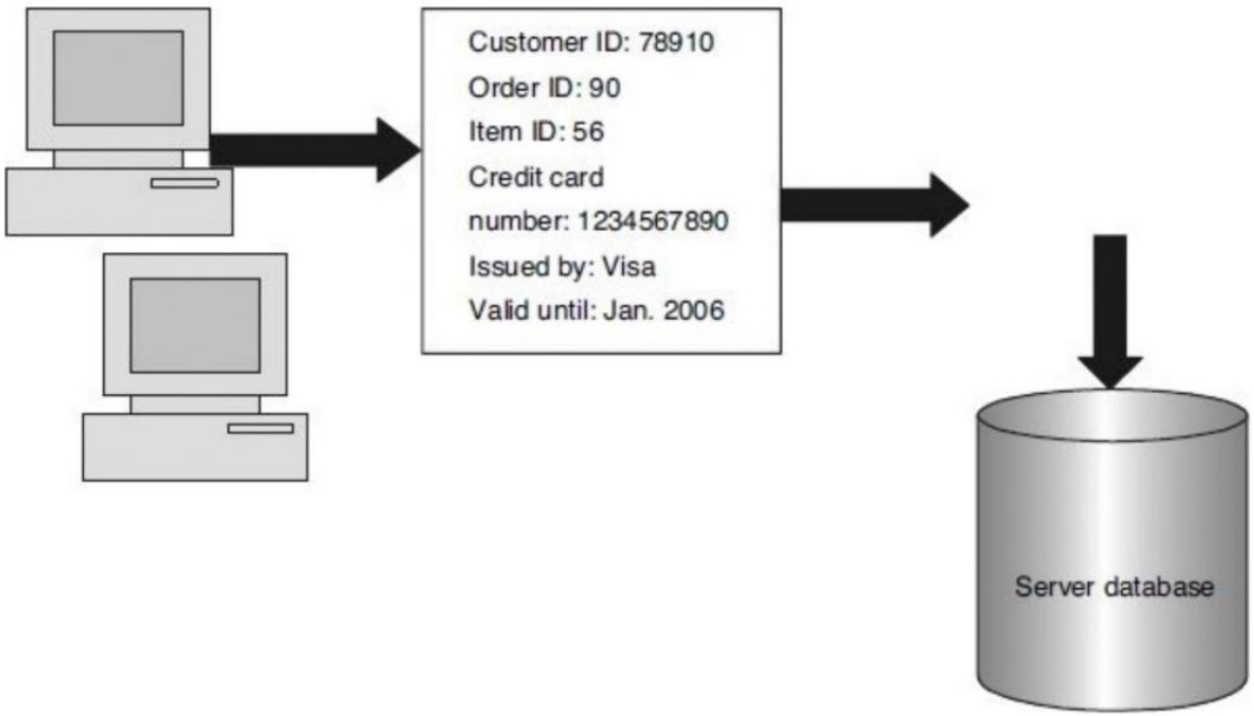
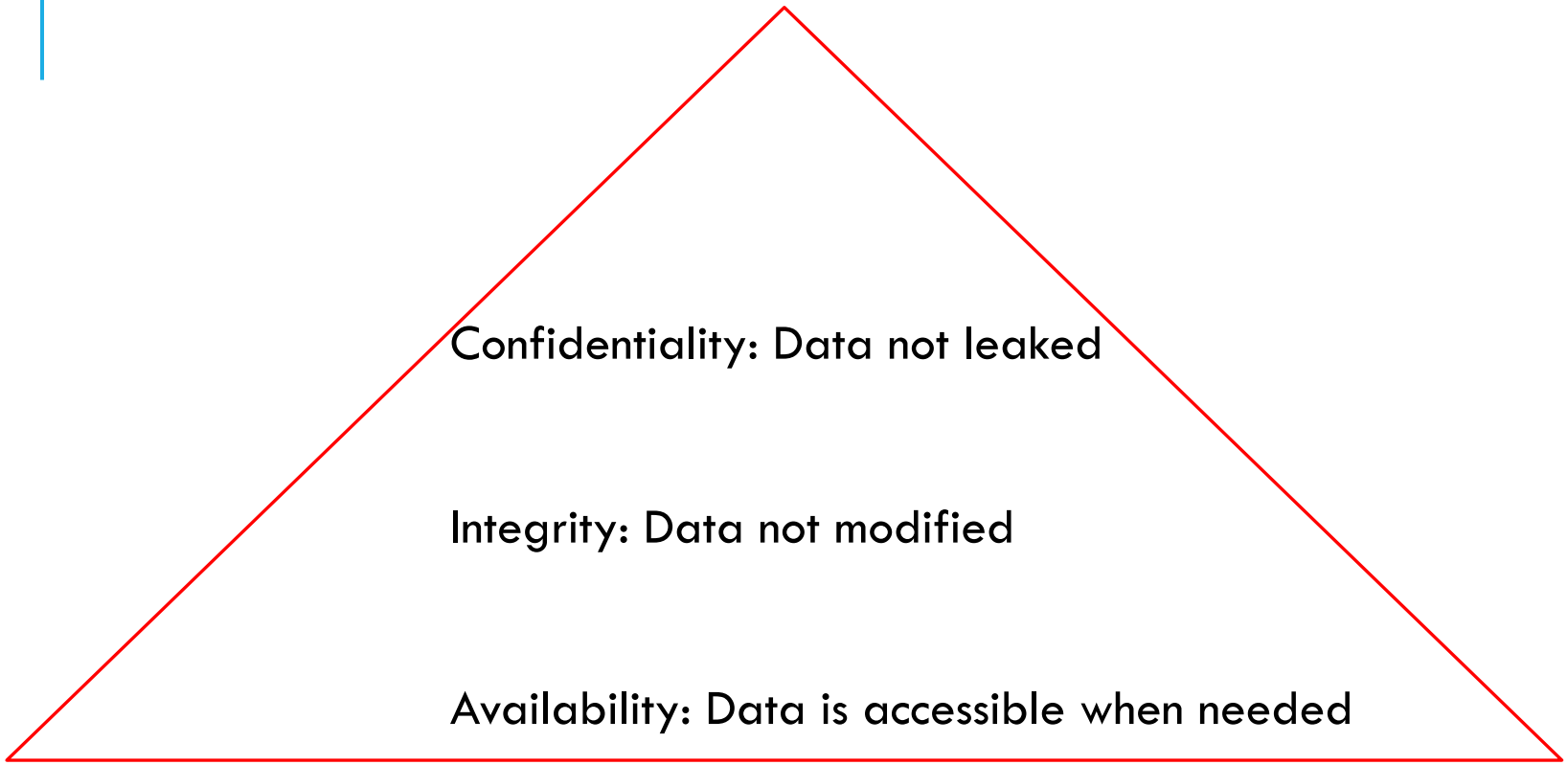


FIGURE 1.1 Example of information traveling from a client to a server over the Internet

KEY SECURITY GOALS (CIA TRIANGLE) (1)



KEY SECURITY GOALS (2)

Confidentiality: Data not leaked

Integrity: Data not modified

Availability: Data is accessible when needed

Authenticity: Data origin cannot be spoofed

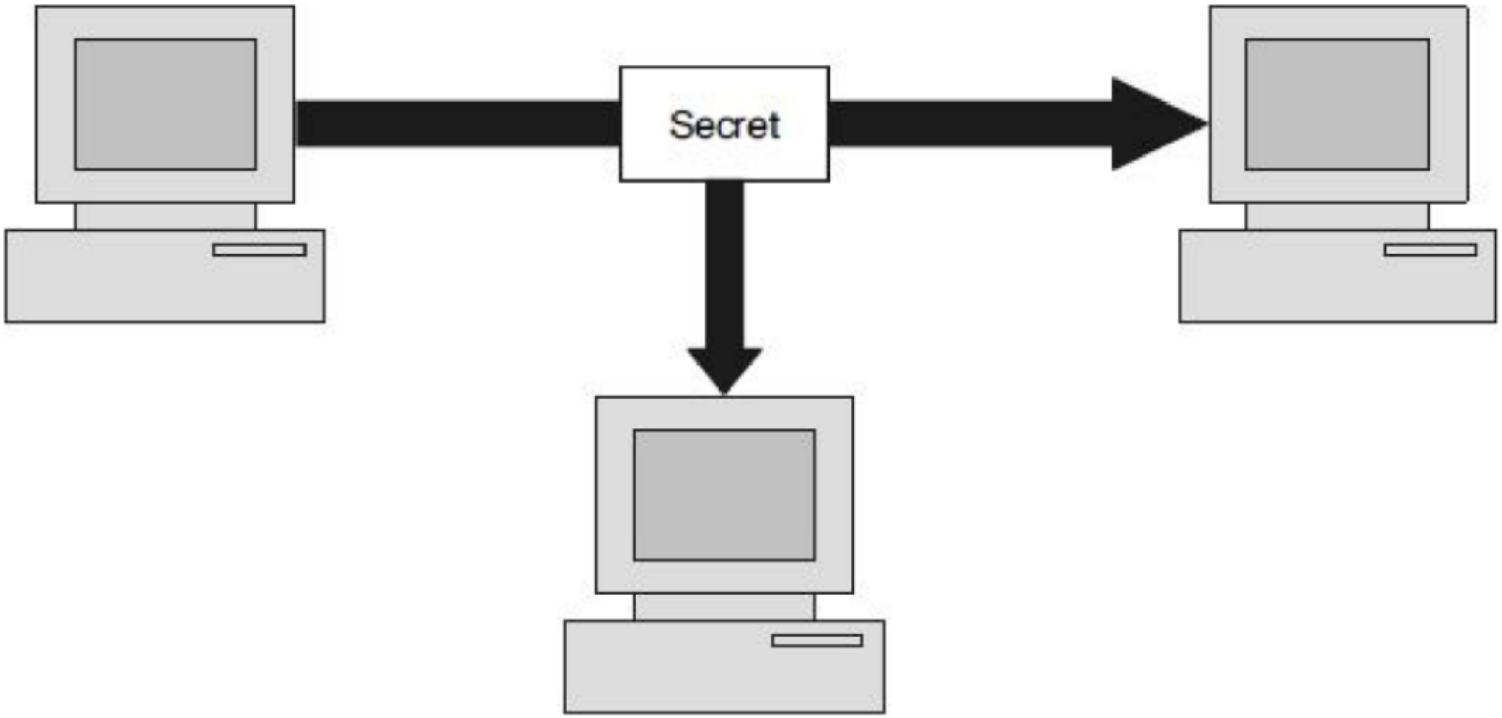


FIGURE 1.2 The loss of confidentiality: Interception causes the loss of the message's confidentiality.

INTEGRITY

When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost.

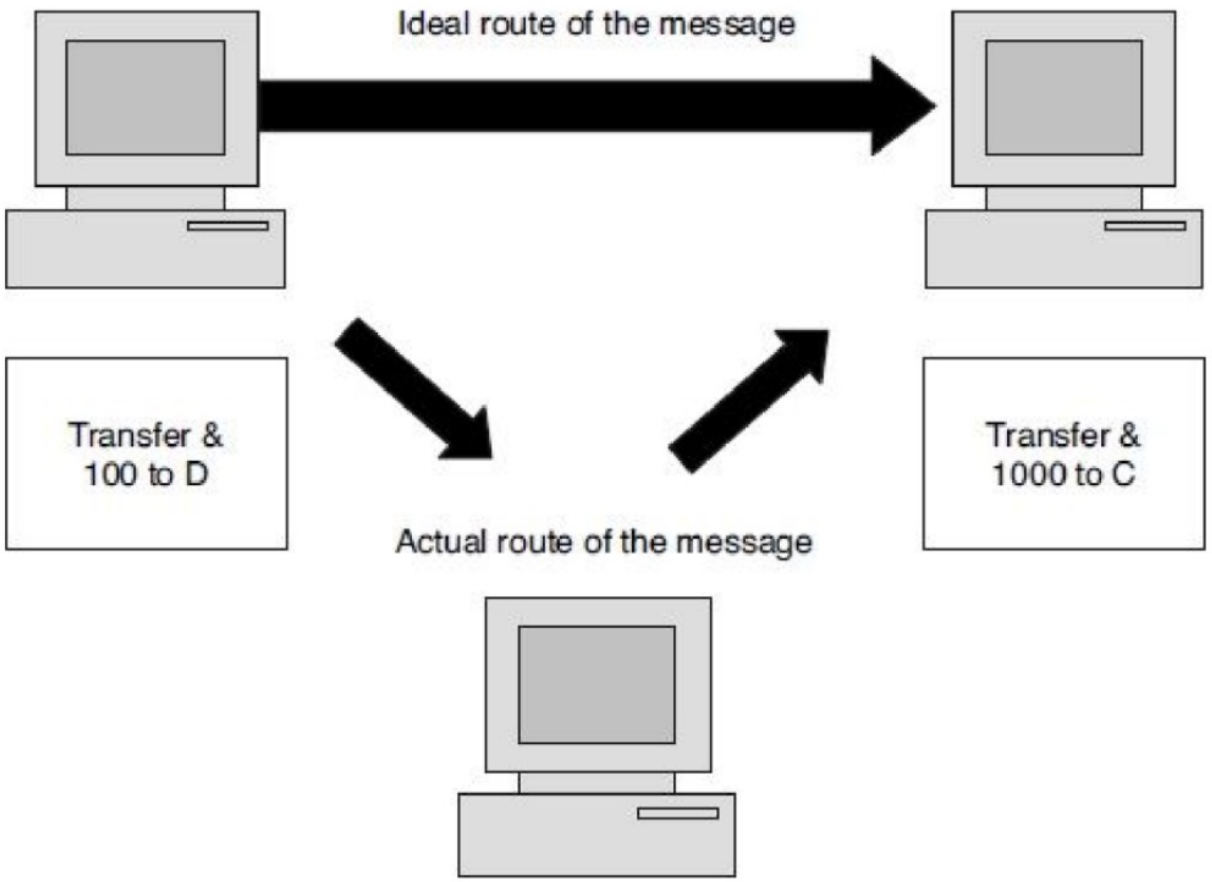


FIGURE 1.4 Loss of integrity

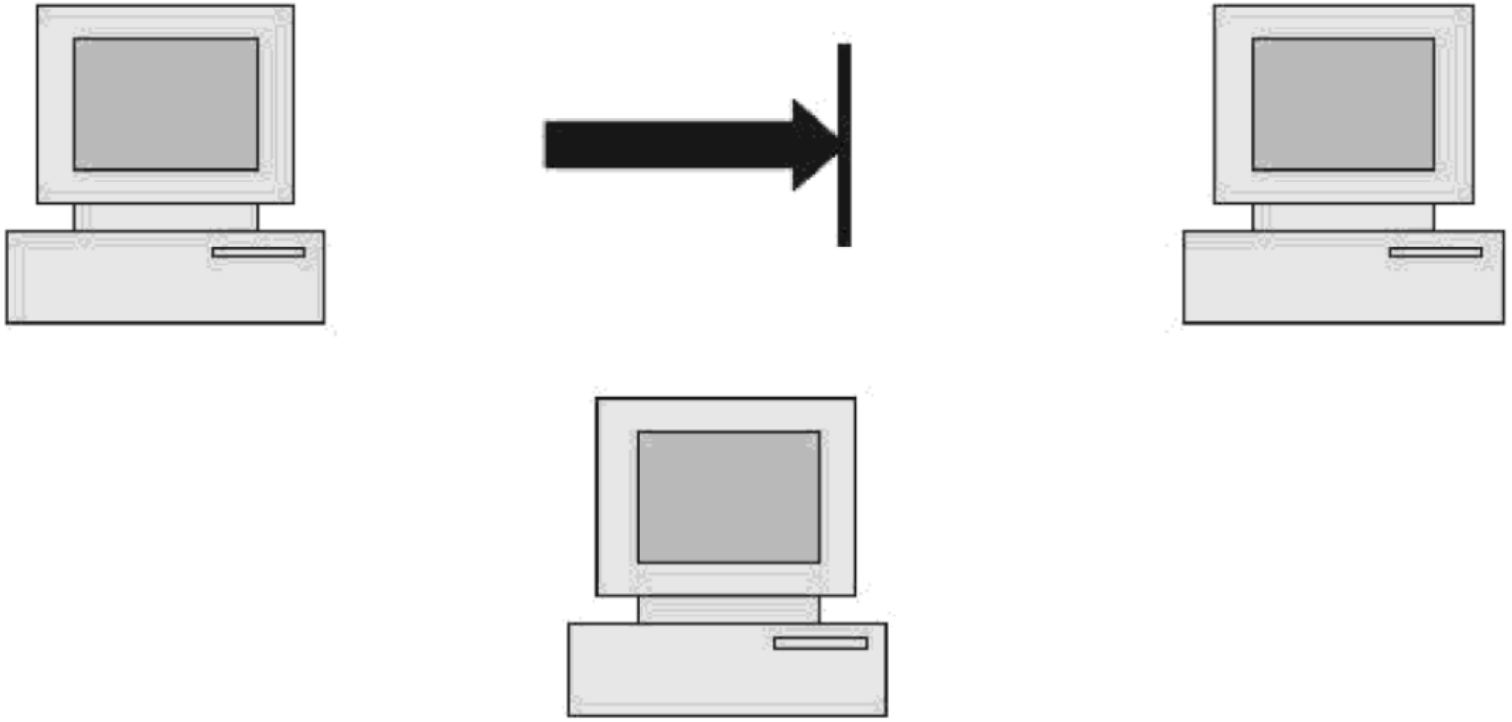


FIGURE 1.5 Attack on availability

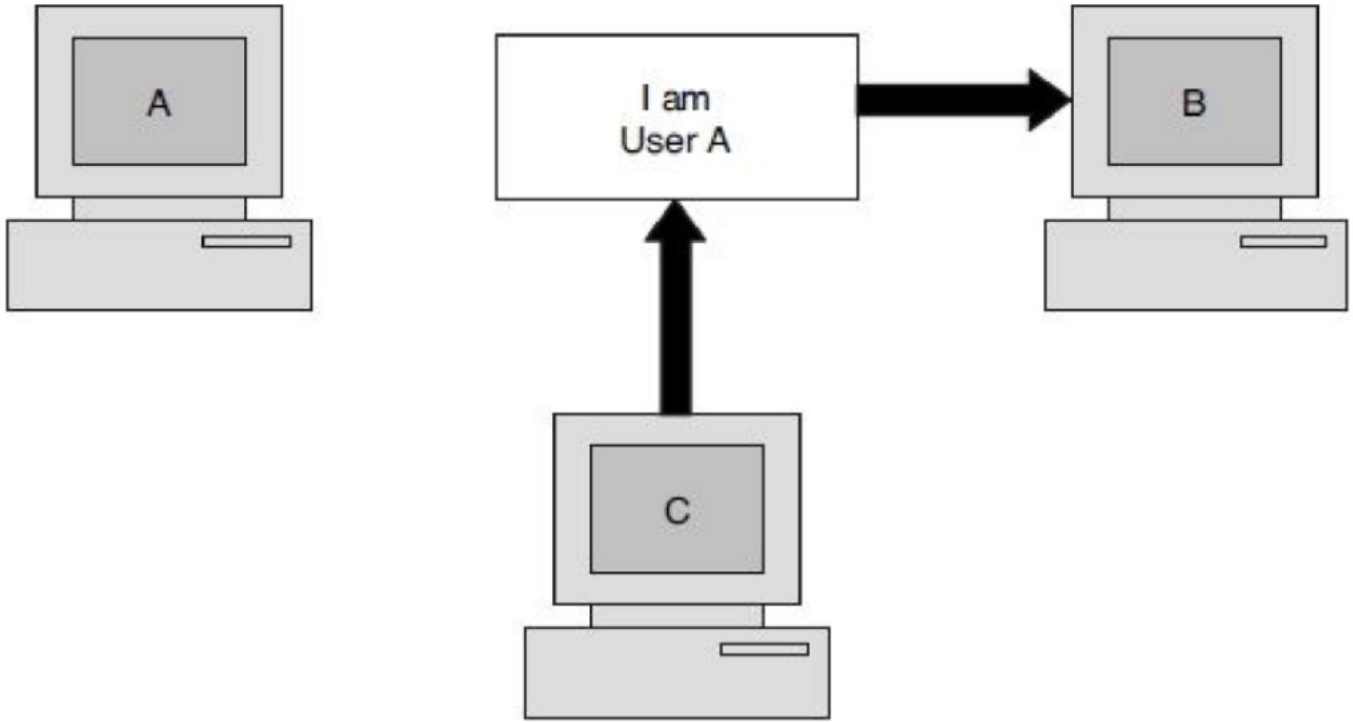


FIGURE 1.3 The absence of authentication

THE ART OF ADVERSARIAL THINKING

WHAT'S ADVERSARIAL THINKING?

"Security requires a particular mindset. Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it."

- Bruce Schneier

ADVERSARIAL THINKING DISCLAIMER

Hopefully, you will learn to think like a criminal mastermind but behave like a gentleman/woman!

ADVERSARIAL THINKING: KEY QUESTIONS

Security goal: what security policy to enforce?

Threat model: who is the adversary? What actions can the adversary perform?

Mechanisms: What security mechanisms can be used to achieve the security goals given the adversarial model

YOU CAN APPLY ADVERSARIAL THINKING ANYWHERE

UNKLAB ID cards

- Can you fake an ID card?

ATM machine

- How does the service person gets access to refill it with cash?

OVO card

- Can you increase the card balance without paying?

YOU CAN APPLY ADVERSARIAL THINKING ANYWHERE

A large company using an old, but deep-rooted mainframe computer used to collect new customer data. Being as old as it is, the mainframe cannot be properly secured, so every weekend the company runs a large migration job that clears out the data off the mainframe and moves it to a secure server.

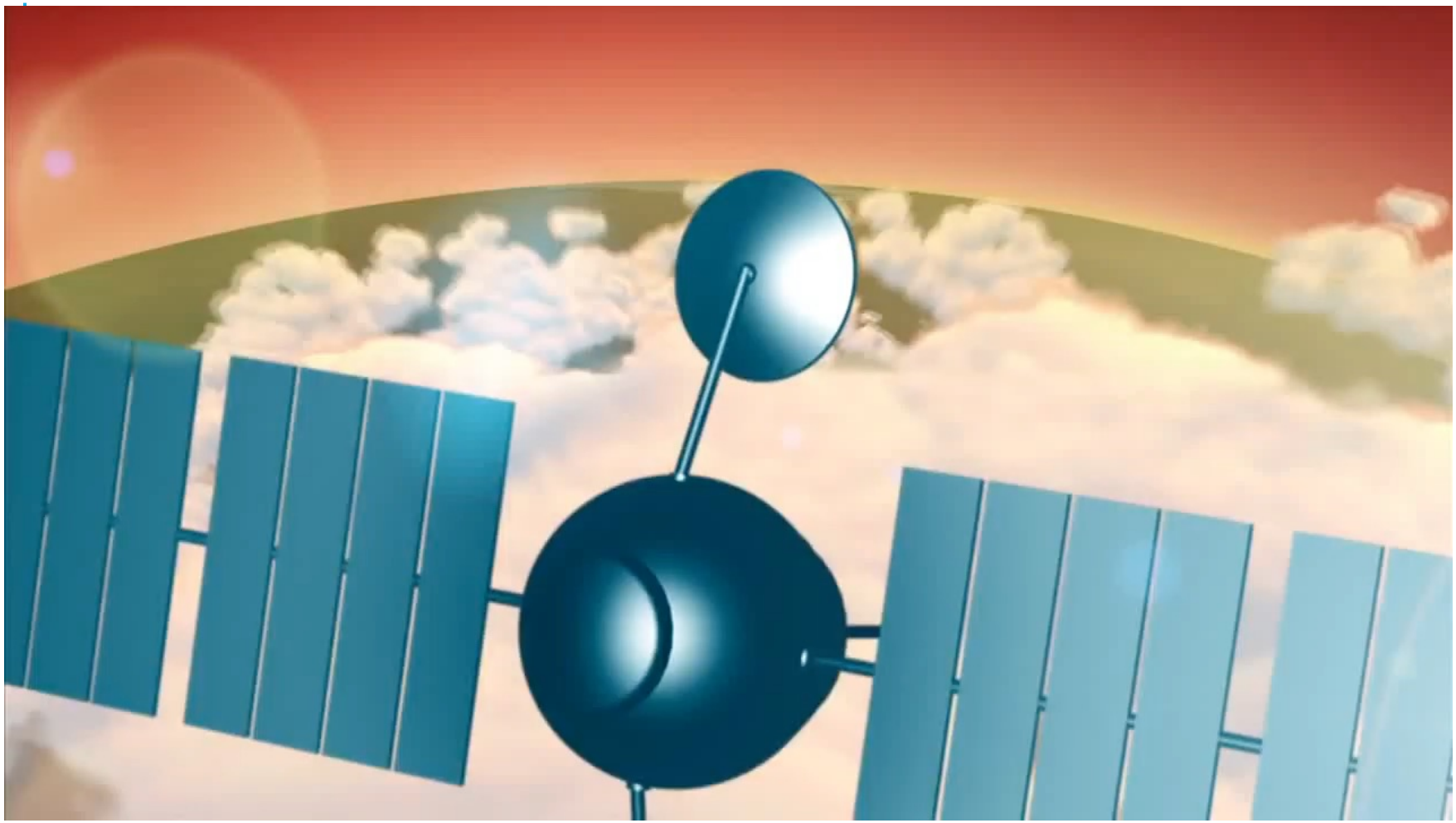
Making bogus bar codes: Just how hard is it?

First it was shoplifting, then it was ticket-switching, and now it's bar code fraud. Just how easy is it to make a fraudulent UPC? Easier than you think. But getting away with the crime is a different story.

Sumi Das May 25, 2012 2:08 PM PDT

Watch this: Making fake bar codes: It's way easier than you think ▶ 1:35

Several San Francisco Bay Area Target stores were the recent, uhhh, target of not one, but two unrelated barcode scammers who apparently found the manufactuer's suggested price of Lego sets too much to bear.



EXAMPLE: AIR TRAVEL

Print boarding pass at home

ID check by TSA

Boarding pass check at the gate

ADVERSARIAL THINKING EXAMPLE: AIR TRAVEL

Security goal: Ensure that each person getting inside an airport has a valid boarding pass and is authorized to fly (i.e., not on the no-fly list)

Mechanisms

- TSA checks validity of the ID (e.g., driver's license) and the boarding pass
- TSA matches name in the ID against the name in the boarding pass
- TSA ensures that the name is not on the no-fly list
- Gate agent checks whether the boarding pass is valid and has been checked by TSA

DHS Traveler Redress Inquiry Program

The DHS Traveler Redress Inquiry Program can provide resolution to travelers with difficulties getting through security and inspection at airport checkpoints, train stations and when crossing U.S. borders.

Learn more and apply for DHS TRIP to resolve travel-related issues if:

- You are unable to print a boarding pass.
- You are denied or delayed boarding a plane.
- You are denied or delayed entry into and exit from the U.S. at a port of entry or border checkpoint.
- You are continuously referred for additional screening at the airport.

No Fly List

The No Fly List is a small subset of the U.S. government Terrorist Screening Database (also known as the terrorist watchlist) that contains the identity information of known or suspected terrorists. This database is maintained by the FBI's Terrorist Screening Center. For more information about the Terrorist Screening Database, visit the Terrorist Screening Center.

TSA is among the U.S. government agencies that screen individuals using information from the Terrorist Screening Database. TSA implements the No Fly List through its Secure Flight program. Individuals on the No Fly List are prevented from boarding an aircraft when flying within, to, from and over the United States.

Can an attacker who is on the no-fly list fly?

WHAT IS THE THREAT MODEL?

Can an attacker create a fake boarding pass?


FRI, MAR 30, 2012

DELTA

Diamond Testacct
GT9549 / SKY PRIORITY

SkyMiles #XXXXXX9718
DIAMOND/ELITEPLUS/SKY CLUB

BOARDING DOCUMENT

JFK ▸ LAX

NYC-KENNEDY (JFK) ▸
Los Angeles (LAX)
FLIGHT DL120

BOARDING 8:20am
GATE* -
ZONE Sky
SEAT 24C
Economy (H)

Depart Fri, 9:00am
Arrive Fri, 12:20pm

*Gates may change. Check airport monitors.

Fly Paperless: www.delta.com/app

Ticket#: 006 2144236059

Can an attacker fake a driver's license?

SECURITY UNDER DIFFERENT THREAT MODELS

Security goal: Ensure that each person getting inside an airport has a valid boarding pass and is authorized to fly (i.e., not on the no-fly list)

- What are the minimum requirements for someone to violate this goal in the current TSA system?
- The current TSA system is secure under which threat models?

NOT ALL THREAT MODELS ARE EQUAL

Which one is harder and why?

- Creating a fake boarding pass
- Creating a fake driver's license

SECURITY MEASURES IN A DRIVER'S L

Security Features

DRIVER LICENSES, PERMITS & ID CARDS

NEW YORK STATE OF OPPORTUNITY. Department of Motor Vehicles

In 2013 New York State began issuing new photo Driver Licenses, Learner Permits, and Identification Cards. The cards provide advanced document security features that help prevent identity theft and protect the owners of the documents. The old style driver licenses will remain valid until the expiration date on the card.

Polycarbonate Material
The cards have a unique metallic sound when dropped on a hard surface.

Anti-copy Ink Colors & Rainbow Printing
The card is manufactured using fine line color graphics that are difficult to reproduce on a color copier or photo printer.

Secondary Photo in Clear Window
The secondary photo is burned into the card with laser engraving. The clear window has clean, beveled edges.

Laser Engraved Photo
The photo is burned into the card on a background of fine line graphics.

Variable Wave Pattern
The "Wave" features the license holder's name as a continuous string of variable sized text which transitions through the clear secondary photo window.

Tactile Laser Engraving
You can feel the raised lettering on the ID number, birth and expiration dates, and signature.

Under Ultra-violet Light
Highly detailed ultra-violet graphics cover the front surface of the card, including a map of NYS, starbursts in the left corner and fine line graphics in the clear window.

C-51A (8/15)

If you have questions regarding the security features or the authenticity of these or any other NYS DMV documents, contact the New York State DMV Division of Field Investigation at: (518) 474-1106.

SECURITY MEASURES IN A BOARDING PASS?

AIR TRAVEL REVISITED: A DIFFERENT SECURITY GOAL

Print boarding pass at home

ID check by TSA

Boarding pass check at the gate

Security goal: everybody boarding an aircraft must pass through TSA security check

EVERYBODY MUST GO THROUGH TSA CHECKS

How does the current TSA system ensure this?

What is an example threat model where this goal can be violated by an attacker?

YET ANOTHER SECURITY GOAL

Only authorized travelers should be allowed to enter premium lounges

- How will the receptionist at the lounge know who is authorized?

WHAT ABOUT TSA PRE-CHECK?

How does TSA Pre-Check work?

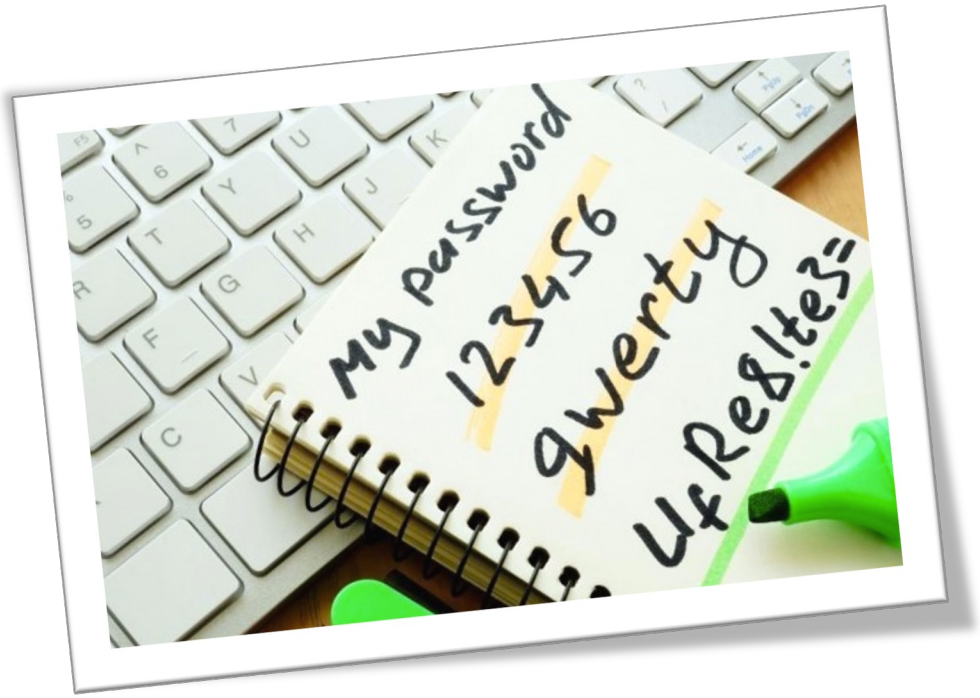
- Passengers apply for Pre-Check
- TSA decide whether the passenger is eligible for Pre-Check or not and sends the information back to the Airline.
- The Airline encodes that information in a barcode that is on the issued boarding pass.

HACKING TSA PRE-CHECK

Source: https://puckinflight.wordpress.com/2012/10/19/security-flaws-in-


s.id

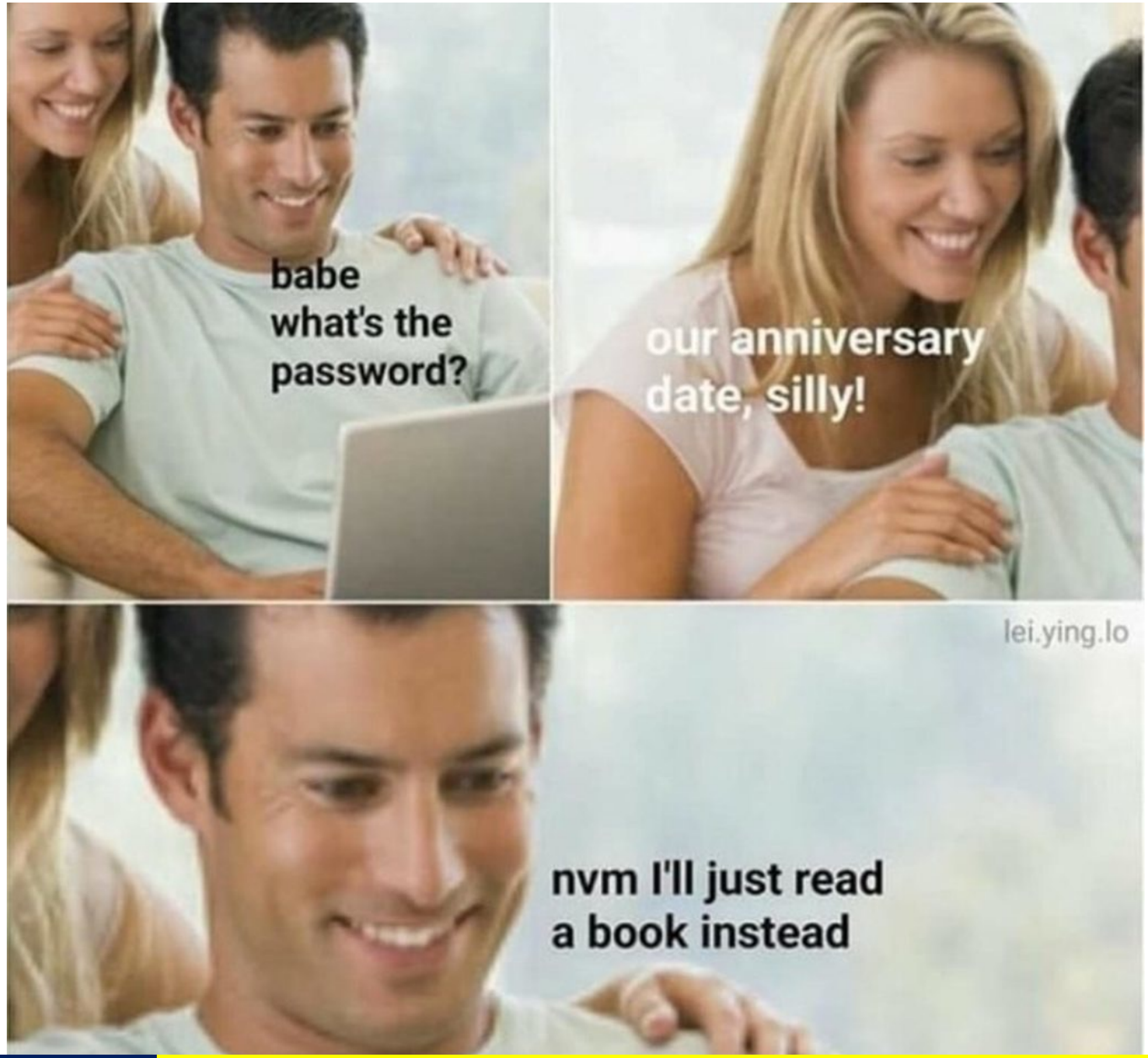
IS YOUR PASSWORD STRONG ENOUGH?




INTERNET
PASSWORD
LOGBOOK
KEEP TRACK OF:
• USERNAMES
• PASSWORDS
• WEB ADDRESSES
IN ONE EASY
&
ORGANIZED LOCATION


SO, WHAT'S YOUR FAVORITE BOOK?
"CALL OF THE WILD" - IT REMINDS ME OF MY OLD DOG
AWW, WHAT'S YOUR DOG'S NAME?
"ROSIE" - ALL THE KIDS IN OUR NEIGHBORHOOD LOVED HER
SPEAKING OF - WHAT STREET DID YOU GROW UP ON?
MAPLE ROAD - WHY DO YOU ASK?
SECURITY QUESTIONS ANSWERED
WELCOME, AMANDA

(Image Courtesy of Shutterstock)


babe
what's the
password?
our anniversary
date, silly!
lei.ying.lo
nvm I'll just read
a book instead

"I created a password and wrote it down like you told me to.
Then I locked it away in a secure folder for safekeeping.
But I need my password to get into the folder!"


I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

DISKUSI

Strongest password in the world

cbvbaby

IS YOUR PASSWORD STRONG ENOUGH?


INTERNET
PASSWORD
LOGBOOK
KEEP TRACK OF:
• USERNAMES
• PASSWORDS
• WEB ADDRESSES
IN ONE EASY
&
ORGANIZED LOCATION


SO, WHAT'S YOUR FAVORITE BOOK?
"CALL OF THE WILD" - IT REMINDS ME OF MY OLD DOG
AWW, WHAT'S YOUR DOG'S NAME?
"ROSIE" - ALL THE KIDS IN OUR NEIGHBORHOOD LOVED HER
SPEAKING OF - WHAT STREET DID YOU GROW UP ON?
MAPLE ROAD - WHY DO YOU ASK?
SECURITY QUESTIONS ANSWERED
WELCOME, AMANDA

(Image Courtesy of Shutterstock)


babe
what's the
password?
our anniversary
date, silly!
lei.ying.lo
nvm I'll just read
a book instead

"I created a password and wrote it down like you told me to.
Then I locked it away in a secure folder for safekeeping.
But I need my password to get into the folder!"


I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."