



ENJOY SAFER TECHNOLOGY™

# Security Day

Joe Wan  
Technical Support Engineer,  
Version2



# Agenda

- Phishing
  - Trend
  - What is Phishing
  - How to prevent
- Mobile Security
  - Risk of weak password
  - How to enhance password security
- Security Password
  - Risk of weak password
  - How to enhance password security
- IoT and Trend

# Phishing

facebook 註冊



您必須登入才可繼續。

登入 Facebook

電郵或電話號碼

密碼

登入

☐ 維持我的登入狀態

[需要幫助?](#) · [註冊 Facebook 帳戶](#)

Luxury Villa in Anglet - H X

tripadvisor.com.vrr6141.top/VacationRentalReview/46f094059c/gaed16c-luxury-villa-in-anglet-...

Apps


tripadvisor Anglet

About Anglet Hotels Holiday Rentals Restaurants Things to do Flights

Holiday Rentals > France > Anglet

### Luxury Villa in Anglet

Overview Reviews Amenities Availability Map



Excellent 8 reviews

from €250 / Night

Book Now

86 travellers viewed this property in the past 24 hours

Send Message

This Property Has Payment Protection

Learn more about paying safely

Overview

Villa - 6 Bedrooms, 7 Bathrooms, Sleeps 12

storeactivepontknitraahlaconnectestor.com/wp-includes/images/wlw/home/websec-login.php

PayPal

### Log in to your account

Email address

Password

Log In

Forgot your email address or password?

Sign Up for Free

All in one pay.  
Pick a card, any card, or bank account, or even apply to get a line of credit from us. It's your money, you choose how to spend it.

Simple. And usually free.  
It's free to sign up for a PayPal account, and we don't charge you a transaction fee when you buy something, no matter how you choose to pay.

About PayPal | Contact Us | Fees | PayPal Developers | Merchant Services | Worldwide | Site Feedback

Privacy | PayPal Blog | PayPal Labs | Jobs | Legal Agreements | Site Map | eBay

Copyright © 1999-2015 PayPal. All rights reserved.



Trip Detail | Expedia

pgapages50.rg-products.com/AirGain\_Pages/17\_Apr\_2018/776637/356\_6744197...

WFD 3.0 examples se

First Price :: 205.71

Expedia

AccountMy TripsSupportEspañol 简体中文

Get DOUBLE points on the app. Learn How

HomeBundle and SaveHotelsCarsFlightsCruisesThings to DoDiscoverVacation RentalsDealsRewardsMobileCollections

Review your trip

Nice Job! You picked one of our cheapest flights.

Book now so you don't miss out on this price!

Tue, May 1

From  
To

Fort Lauderdale - Hollywood Intl. (FLL)  
Toussaint Louverture Intl. (PAP)

Cheapest

Spirit Airlines

7:15am  
FLL

→

9:14am  
PAP

1h 59m, Nonstop

Show flight and baggage fee details

Tue, May 8

From  
To

Toussaint Louverture Intl. (PAP)  
Fort Lauderdale - Hollywood Intl. (FLL)

Cheapest

Spirit Airlines

10:17am  
PAP

→

12:24pm  
FLL

2h 7m, Nonstop

Show flight and baggage fee details

Change flights

Buy this flight & you'll earn exclusive hotel deals!

Continue Booking

Save this Itinerary

Trip Summary

Traveler 1: Adult \$205.71  
Booking Fee \$0.00

Trip Total: \$205.71

Rates are quoted in US dollars

66965 customers protected their flight in the last 7 days. Add flight protection when you check out.

Important Flight Information

Tickets are non-refundable and non transferable. A fee of \$125.00 per ticket is charged for itinerary changes. Name changes are not allowed.

All Spirit Airlines fares are nonrefundable

Spirit's low Bare Fares™ get you from A to B with a free personal item (such as a purse or small backpack) that must fit underneath your seat (Maximum dimensions: 18"x14"x8")

Additional purchases required for:

One carry-on bag per passenger

All checked bags (over-weight charges apply starting at 41 lbs)

Advance seat assignments

All onboard drinks and snacks

For the full pricing list, please visit: Spirit Airlines

Earn 25,000 Expedia Rewards bonus points

after qualifying purchases with the Expedia Rewards Voyager Credit Card from Citi.

Learn more and apply

Review Trip Details and B

pgapages50.rg-products.com/AirGain\_Pages/17\_Apr\_2018/776637/70\_6

WFD 3.0 examples se

Payment Info (Secure SSL Encrypted Transaction)

Payment Method Select

Credit or Debit Card Number

Card Holder's Name

Expiration Date Month Year

Card Verification Number

(Pay with credit or debit card)

(As it appears on your credit card)

3 digit number from your card

Payment Acceptance Policy Privacy Policy Safe Shopping Guarantee

Norton Secured powered by VeriSign

Billing & Contact Information

Credit Card Billing Address:

Country United States

Street

City (example: Chicago)

State Select

Zip

Contact Information :

Phone Number In case we need to reach you

I agree to receive text alerts and calls about this trip. See details

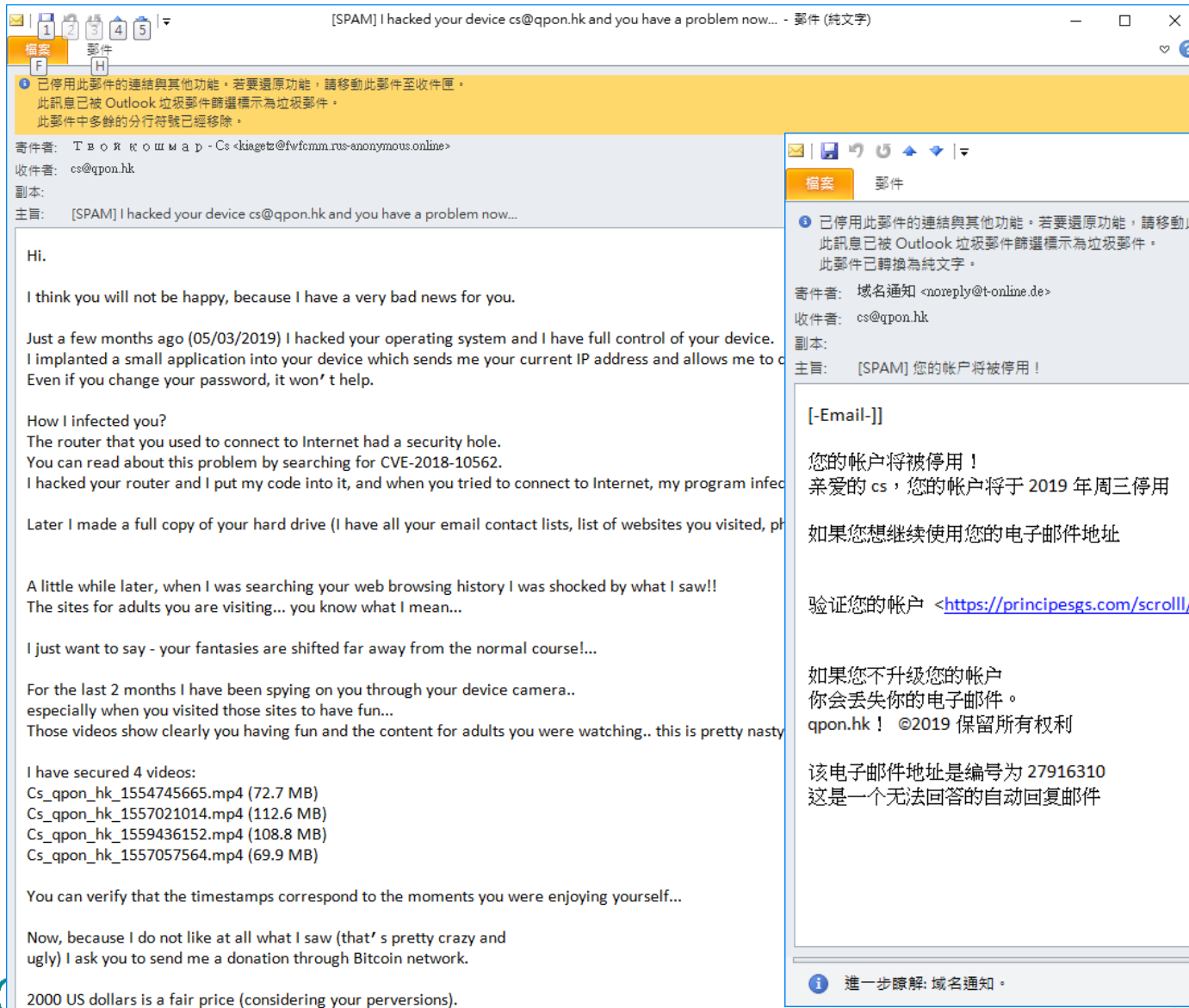
Email

Retype Email

# Phishing in other media



# Phishing in Email



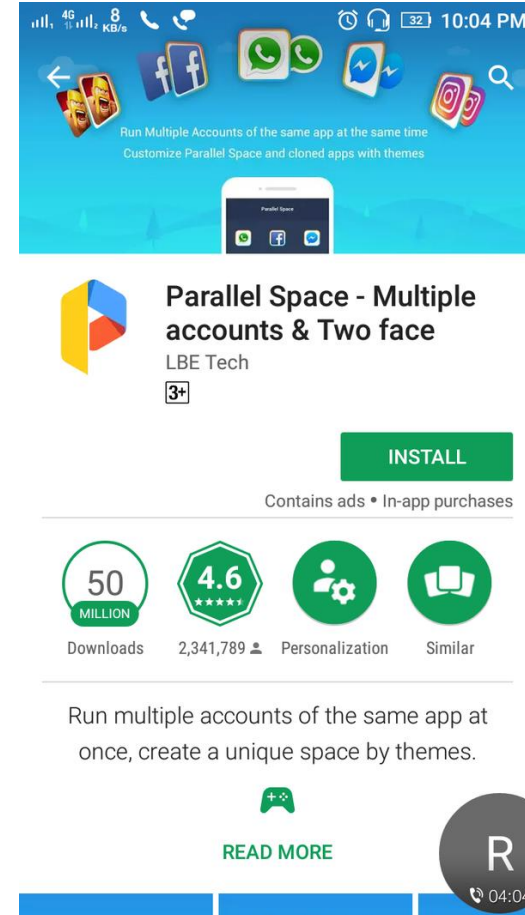
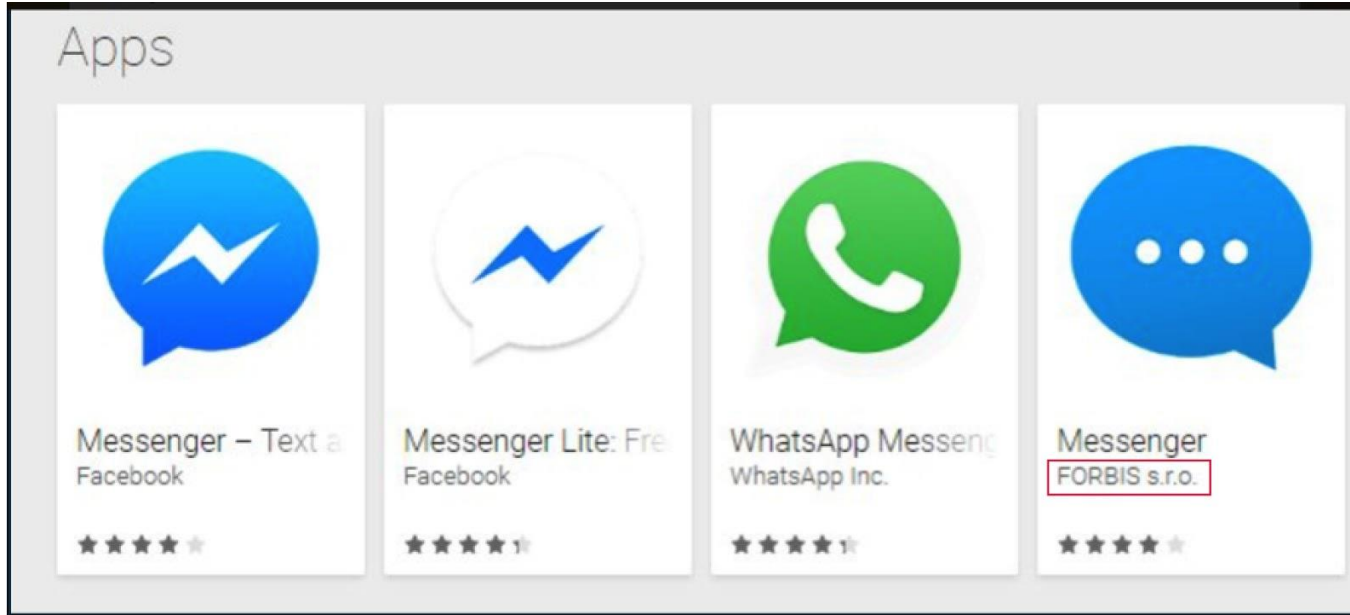


# Phishing Apps On Mobile

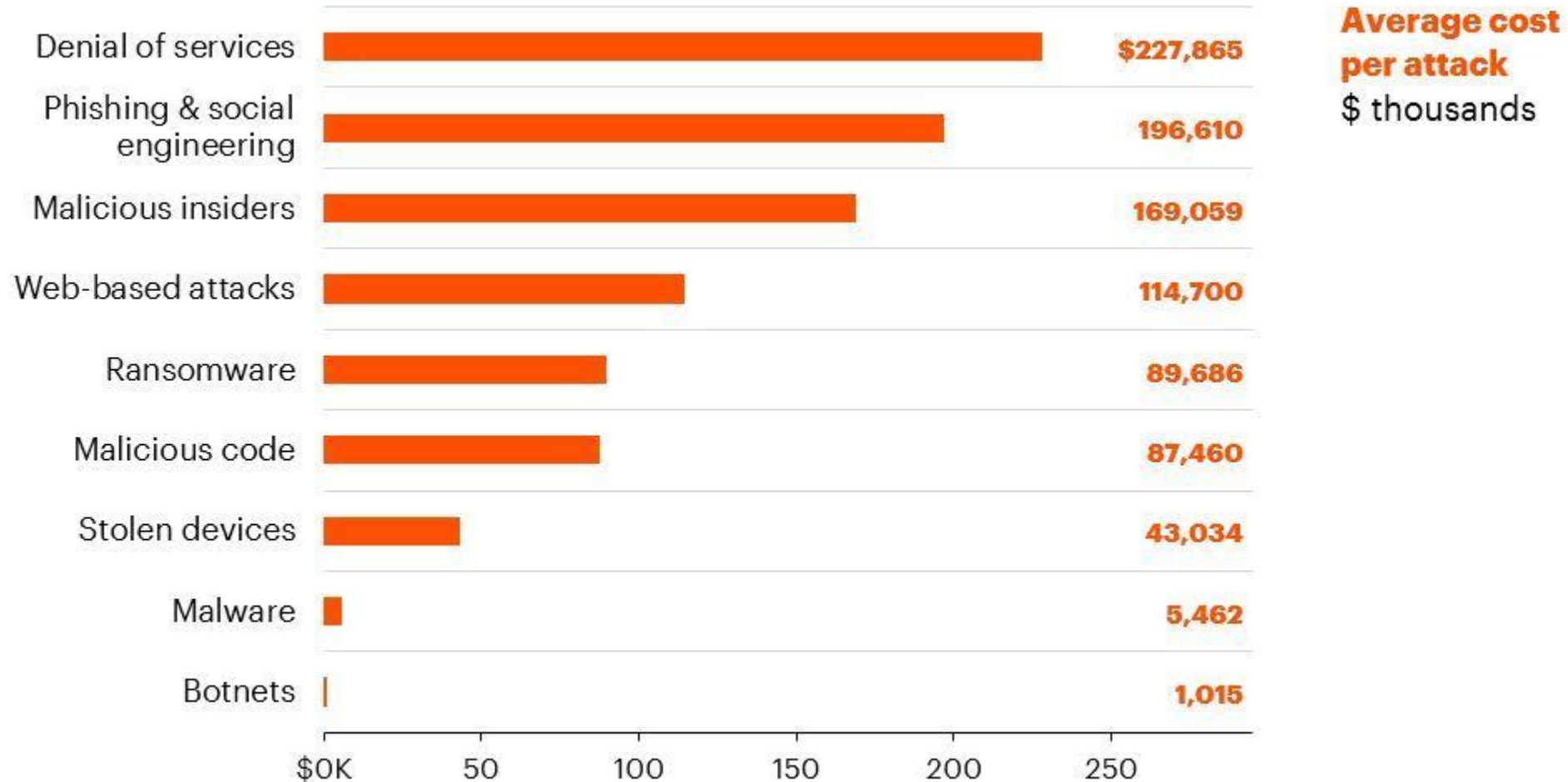


(Graphic: quick heal)

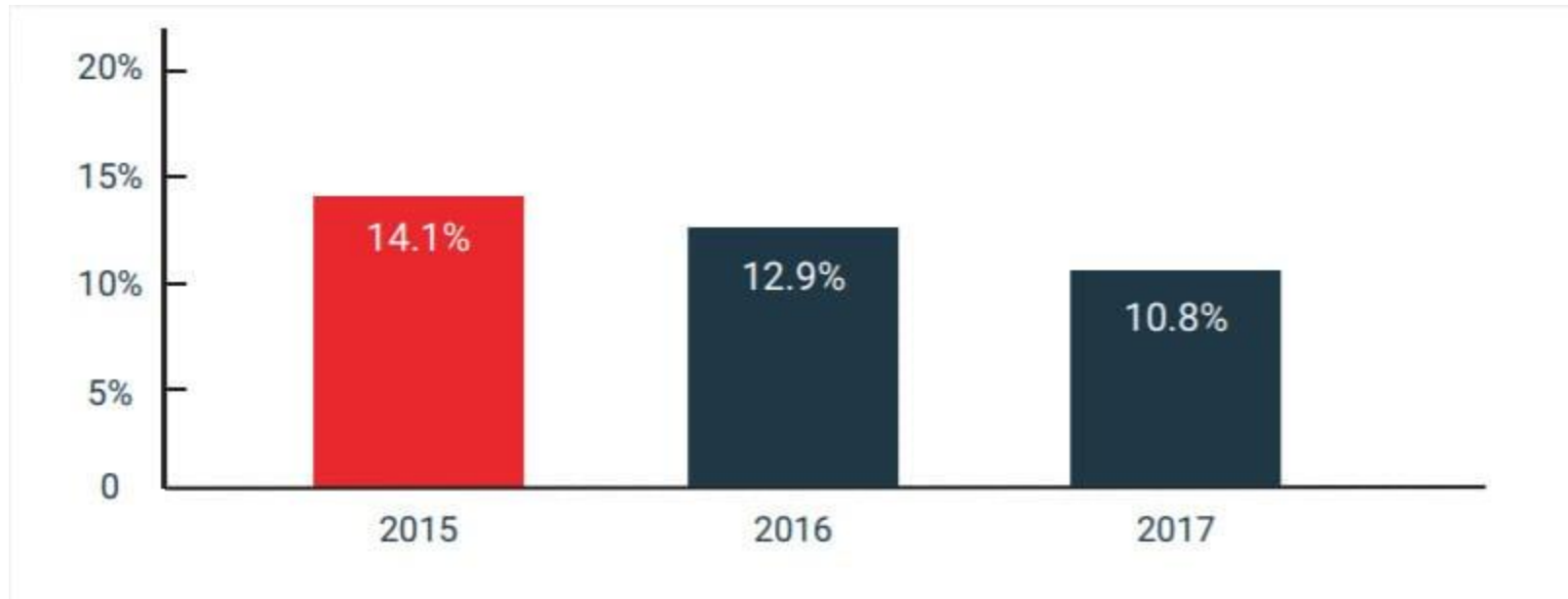
# Even More



# Most Costly Attack Types for Financial-Services Firms (US 2017)



# Phishing Trend (World)



# How to prevent phishing?

- Check the email sender address when receiving email
- Check that the website's address seems to be genuine by looking for subtle misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have.
- Do not click any suspicious hyperlink
- Confirm and verify the web-site/email/message/etc. identification and authenticity
- Using Secure browser for online financial-services access



# Mobile Security

# Mobile hacking



## To improve mobile security

- Beware the phishing attack
- Check the access right before installing or updating app, do not accept or install if the function access is not reasonable, such as: PDF viewer tool require full access of contact list, phone access, location access, etc.
- Do not install app from unknown source
- Avoid to open suspicious files
- Avoid to access non-safe WiFi connection

# Security With Password

# What is password

A password is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource

(Source: Wikipedia)





# 2018's worst passwords

- |              |              |               |
|--------------|--------------|---------------|
| 1. 123456    | 10. iloveyou | 19. 654321    |
| 2. Password  | 11. princess | 20. !@#\$%^&* |
| 3. 123456789 | 12. admin    | 21. charlie   |
| 4. 12345678  | 13. welcome  | 22. aa123456w |
| 5. 12345     | 14. 666666   | 23. donald    |
| 6. 111111    | 15. abc123   | 24. password1 |
| 7. 1234567   | 16. football | 25. qwerty123 |
| 8. sunshine  | 17. 123123   |               |
| 9. qwerty    | 18. monkey   |               |

# Risk of weak Password



“Passwords will always be the single biggest failure point of any network or login.

Simple password cracking procedures will take data that’s been hacked and leaked, match it against a known word and bingo they now have your password”

(Source: Interview with Mark James, ESET IT security specialist)

# How to enhance security on password?

- Do not use the simple password combination, such as: P@ss0rd, 98765432, etc.
- Don't use part of your login name or your personal data(e.g.: Phone number, birthday, etc.) in your password
- Using different password on difference devices/web-site/login/etc.
- Change password regularly

# How to enhance security on password?

- Do not rely on password managing application or physical memo-note to save all password
- When entering your password, be aware of your surroundings
- Enhance password security with “Two Factor Authentication” if possible

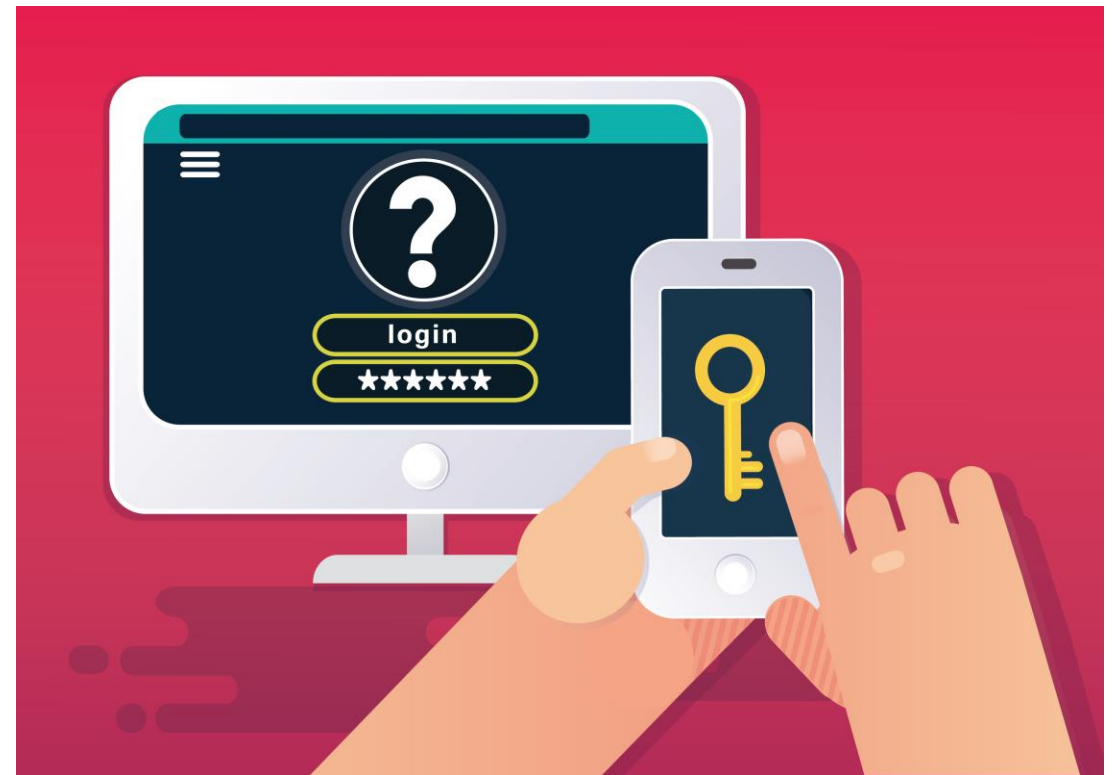
# How to enhance security on password?

- Do not rely on password managing application or physical memo-note to save all password
- When entering your password, be aware of your surroundings
- Enhance password security with “Two Factor Authentication” if possible



# What is Two Factor Authentication (2FA)

- The most advance and secure solution for password security
- A solution to prevent single password compromises
- Preventing password hacking such as brute-force, dictionary or rainbow table attacks



# Examples of 2FA

**UNITED**  
Mileage Plus®

**Verified by**  
**VISA**

**Protect Your Visa Card Online**

Verified by Visa protects your Visa card against unauthorized use online - **at no additional cost**. For details, [click here](#).

To use Verified by Visa on this and future purchases, complete this page. You'll then create your own Verified by Visa password.

Your Social Security Number (last 4 digits): XXX - XX -

Signature Panel Code:   The last 3 digits on the back of your card ([more help](#))

Expiration Date:  /  (MM/YY)

E-mail address:  How will it be used?

[Sign up to complete purchase](#)

By activating now, you agree to the Chase [Terms of Use](#).  
[Click here](#) to view Chase Privacy Policy.  
Note: The data you provide to Chase is secure and is only used to help verify your identity.

1. Enter your phone number here

2. Click here to send the SMS

3. Check your phone for the code

4. Enter the code here

5. Fill out the rest of the form

**会員情報入力**

入力 確認 完了

ログインID  [必須](#)

メールアドレス  
test@epius.co.jp

携帯電話番号 (半角数字) (ハイフン不要)  
例: 090\*\*\*\*\*

携帯電話番号を入力して「認証番号を送信」ボタンを押し、携帯電話 (SMS) に届いた認証番号を入力してください。認証番号の送信後、5分以内に会員情報の入力を完了してください。

携帯電話番号 (SMS) 認証について ⓘ

[認証番号を送信](#)

認証番号 (半角数字) 例: 0000 [必須](#)

8文字以上16文字以下  
確認のための再度入力してください。  
8文字以上16文字以下

名前 (全角) [必須](#)

(姓) 例: 山田 (名) 太郎

(セイ) 例: ヤマダ (メイ) タロウ

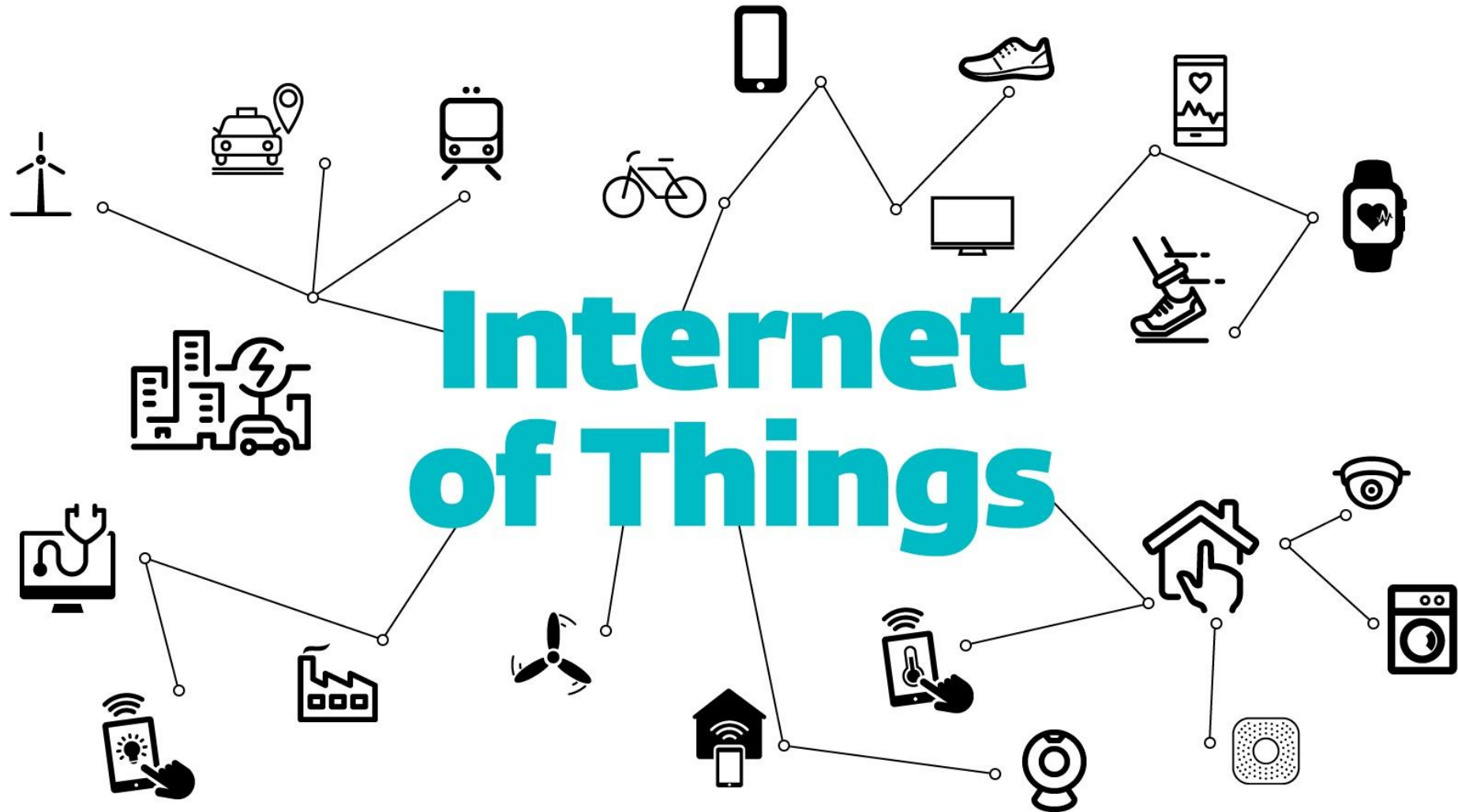
郵便番号 (半角数字) (ハイフン不要) [必須](#)

例: 1506005

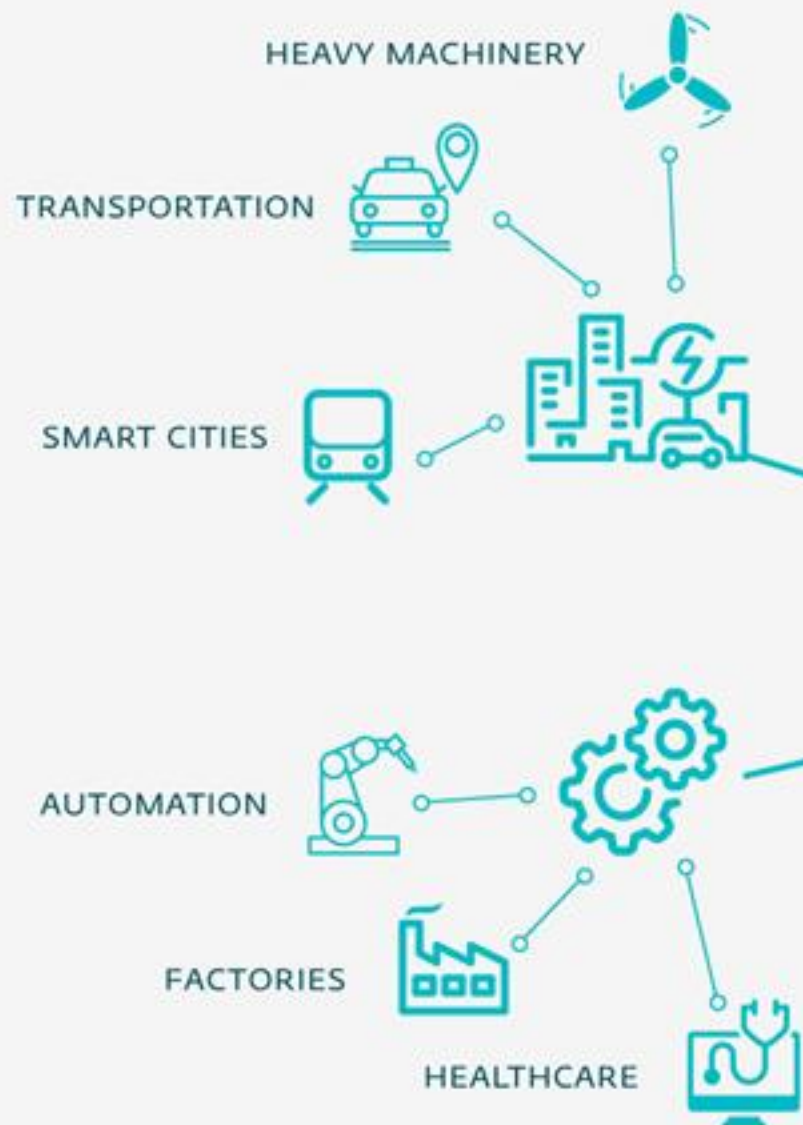
住所とクレジットカード登録 [+](#)

# IoT

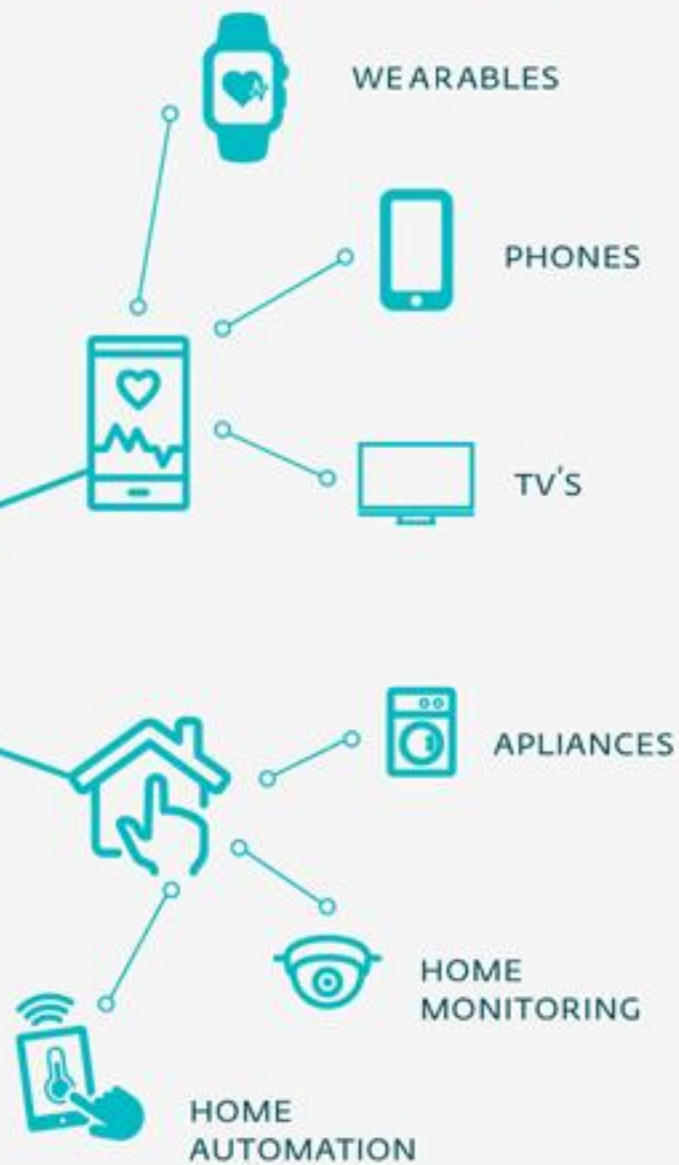
What is it?



## INDUSTRIAL IoT

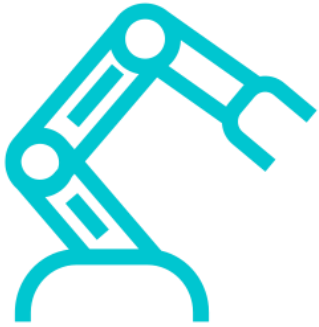


## CONSUMER IoT





# Views on the Internet of Things?



Industrial  
Automation



Smart  
Health



Smart  
Home



Smart  
City

# Views on the Internet of Things?



Late 1970's

## X10

by Pico Electronics

**THE X-10 POWERHOUSE  
INTERFACES WITH YOUR COMMODORE  
TO CONTROL YOUR HOME...FOR SECURITY,  
COMFORT AND ENERGY SAVINGS.**

This remarkable Interface lets you run your home through your Commodore 64 or 128 and a keyboard or joystick.

When you're away, it makes your home look and sound lived in. When you're home, it can turn off the TV at night and wake you up to stereo and fresh brewed coffee in the morning. It can condition and control your heating.



and then p...  
The Interfac...  
ules through...  
interfere with n...  
appliances.

There are plug-in App...  
Lamp Modules, Wall Sw...  
Modules and Special 220V Mo...  
heavy duty appliances such as water...  
heaters and room air conditioners. Plus Thermostat Controllers  
for central heating and air conditioning. Telephone Responders  
to control your home from any phone, and much more.

**IT WON'T TIE UP YOUR COMPUTER.** Use your computer only  
when you're finished, disconnect the Inter-...  
ed into...

# IoT Failures



# Smart phones

- Original iPhone, 29 June 2007 (USA)
- Oct/Nov 2009 “Dutch hack”
- Only jailbroken phones
- Abused default SSH password
- Changed device wallpaper
- Asked for €5 “ransom”



# Smart phones

- First Android phone, 22 Oct 2008 (USA)
- Aug 2010 Android/FakePlayer.A
- Fake media player app
- From Russian porn sites
- Sent premium-rate SMSes



# Smartwatch security fails to impress: Top devices vulnerable to cyberattack

A new study into the security of smartwatches found that 100 percent of popular device models contain severe vulnerabilities.



By [Charlie Osborne](#) for [Zero Day](#) | July 22, 2015 -- 17:25 GMT (03:25 AEST) | Topic: [Security](#)



Apple

A research study conducted by Hewlett-Packard has found serious security issues in today's top smartwatch wearable devices.

Smartwatches are part of the wearable device trend, which extends from medical devices and fitness trackers to acting as an extension of your smartphone.

The [Apple Watch](#) and [Android Wear](#) are examples of popular wearable devices on the market which can pair with smartphones and allow you to view online notifications, send messages and control apps through either the small display or through voice control.

Wearables can be useful and have grown in popularity with the arrival of the Internet of Things (IoT) concept in the marketplace. However, as smartwatches become mainstream,

[Home](#) > [Security](#)



## SECURITY IS SEXY

By [Darlene Storm](#), Computerworld | JUL 7, 2016 8:27 AM PT

### About

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

### NEWS ANALYSIS

# Hackers can exploit smartwatches, fitness trackers to steal your ATM PIN

Smartwatches and fitness trackers can be exploited to give attackers your ATM PIN and passwords.







6-DAY

# Samsung's Tizen said to be riddled with vulnerabilities. Is your smartwatch safe?

BY JERRY HILDENBRAND Tuesday, Apr 4, 2017 at 7:00 am EDT



25 Comments

A report from Motherboard is some very bad news for fans of Samsung's *other* operating system, Tizen.

Speaking with Israeli security researcher *Amihai Neiderman* of [Equus Software](#), [Motherboard](#) tells us that there are currently 40 unreported security vulnerabilities that would allow remote execution and hacking of every Samsung TV, watch or phone that uses [Tizen](#) as the operating system. More serious are some allegations about the how and why behind many of these exploits.

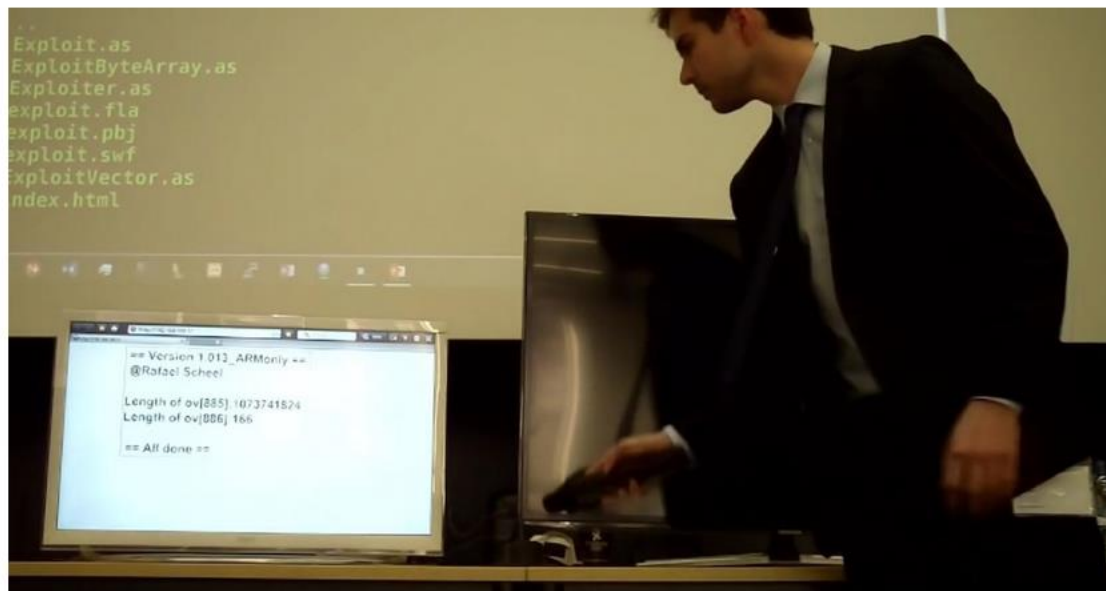
It may be the worst code I've ever seen.

While Samsung may not be thinking about replacing Android with Tizen on its phones and tablets, the current ecosystem is about to be expanded in a big way: Samsung is committed to using Tizen on most every smart appliance it sells going forward. Smart refrigerators sound like a great idea until someone hacks your email through one.

## About 90% of Smart TVs Vulnerable to Remote Hacking via Rogue TV Signals

By [Catalin Cimpanu](#)

March 29, 2017 01:30 PM 4



A new attack on smart TVs allows a malicious actor to take over devices using rogue [DVB-T](#) (Digital Video Broadcasting — Terrestrial) signals, get root access on the smart TV, and use the device for all sorts of nasty actions, ranging from DDoS attacks to spying on end users.

The attack, developed by Rafael Scheel, a security researcher working for Swiss cyber security consulting company [Oneconsult](#), is unique and much more dangerous than previous smart TV hacks.

### Current smart TV hacks aren't not really "dangerous"

Until now, all smart TV exploits relied on attackers having physical access to the device, in order to plug in an USB that executes malicious code. Other attacks relied on social engineering, meaning attackers had to trick users into installing a malicious app on their TV.



DEPARTMENT OF JUSTICE  
FEDERAL BUREAU OF INVESTIGATION  
FBI HEADQUARTERS

WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION «THE LEGAL BASIS OF VIOLATIONS». ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.

THE SIZE OF THE PENALTY IS **\$500.00**

**ATTENTION!**

DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON-PAYMENT IN A CURRENT OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.

TO MAKE A PENALTY PAYMENT, GO TO SECTION «PAYMENT PENALTIES»



DIRECTOR JAMES COMEY  
FEDERAL BUREAU OF INVESTIGATION  
935 PENNSYLVANIA AVENUE, N.W.  
WASHINGTON, DC 20535-0001



# HAPI.com



**HAPIfork**  
by Jacques Lépine

Eat slowly.  
Lose weight.  
Feel great!

**Buy now**

**50% OFF** ~~US\$ 99~~ **US\$ 49**

**slow control!**

**2013**

**BEST OF CES 2013**

**FINALIST**

**PC**

**CES**

## HAPIfork: Eat slowly, lose weight, feel great!



Eating too fast leads to poor digestion and poor weight control. The HAPIfork, powered by [Slow Control](#), is an electronic fork that helps you monitor and track your eating habits. It also alerts you with the help of indicator lights and gentle vibrations when you are eating too fast. Every time you bring food from your plate to your mouth with your fork, this action is called: a **"fork serving"**. The HAPIfork also measures:

- \* How long it took to eat your meal.
- \* The amount of "fork servings" taken per minute.
- \* Intervals between "fork servings".

This information is then uploaded via USB or Bluetooth to your Online Dashboard on HAPI.com to track your progress. The HAPIfork also comes with the HAPIfork and HAPI.com apps plus a coaching program to help improve your eating behavior.

Gadget

# Germany tells parents to destroy microphone in 'illegal' doll

by Alanna Petroff @AlannaPetroff

🕒 February 17, 2017: 12:09 PM ET

Germany's telecommunications regulator has warned parents that a doll sold in the country could be used to snoop on families and compromise their personal information.

The regulator has recommended that parents immediately stop use of the "illegal" doll and destroy its internal microphone.

The doll -- called My Friend Cayla -- connects to the internet via Bluetooth. The setup allows it to listen and respond to questions like: "What's the tallest animal in the world?" (Answer: Giraffe)

But the German regulator says the doll's design violates privacy rules. They worry that it could be used to snoop on families.

"The ownership of this device is illegal," said Olaf Peter Eul, a spokesman for the country's telecoms regulator. "We expect people to act as lawful citizens and destroy the functionality of the doll."







# This doll recorded kids' conversations without parental consent

*Security experts found ways to listen in*

by [Ashley Carman](#) | [@ashleyrcarman](#) | Dec 8, 2016, 11:36am EST



Photo by Rob Stothard/Getty Images

Two connected toys — the [My Friend Cayla](#) doll and [i-Que Intelligent Robot](#) — allegedly violated kids' privacy protections by recording their conversations without parental consent, according to [a complaint](#) sent to the FTC this week. Both connected toys, from manufacturer Genesis Toys, ship with a built-in Bluetooth microphone and speaker to facilitate communication between kids and the toys' companion iOS / Android app. Both also search



# Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings



LORENZO FRANCESCHI-BICCHIERAI  
Feb 28 2017, 10:00am

**A company that sells “smart” teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.**

**UPDATE, Feb. 28, 12:25 p.m. ET:** After this story was published, a security researcher revealed that the stuffed animals themselves could easily be hacked and turned into spy devices.

A company that sells internet-connected teddy bears that allow kids and their far-away parents to exchange heartfelt messages left more than 800,000 customer credentials, as well as two million message recordings, totally exposed online for anyone to see and listen.

Since Christmas day of last year and at least until the first week of January, Spiral Toys left customer data of its CloudPets brand on a database that wasn't behind a firewall or password-protected. The MongoDB was easy to find using Shodan, a search engine makes it easy to find unprotected websites and servers, according to several security researchers who found and inspected the data.

The exposed data included more than 800,000 emails and passwords, which are secured with the strong, and thus supposedly harder to crack, hashing function bcrypt. Unfortunately, however, a large number of these passwords were so weak that it's possible to crack them, according to Troy Hunt, a security researcher who maintains Have I Been Pwned and has analyzed the CloudPets data.

Buy Now





# A Smart Pump Used By Hospitals To Deliver IV Drugs Is Vulnerable To Wireless Attacks

Dell Cameron

Sep 12, 2017, 6:00pm · Filed to: cybersecurity ▼

Share f T in J u



The last place you should have to worry about being hacked is laid out in a hospital bed. But as wireless devices continue to fill patient rooms, those fears can't help but grow.

Photo: Getty

Last week, the US Department of Homeland Security (DHS) issued an advisory warning about a vulnerability unearthed in one such wireless device. Security researcher Scott Gayou identified eight vulnerabilities in a syringe infusion pump -- a machine used to administer to patients precision doses of medication intravenously.

# 465,000 Patients Need Software Updates for Their Hackable Pacemakers, FDA Says

A painful reminder that a future where the internet is in every device—even the most critical one—can be disastrous.

[SHARE](#)[TWEET](#)

Lorenzo Franceschi-Bicchierai

Aug 31 2017, 2:53am

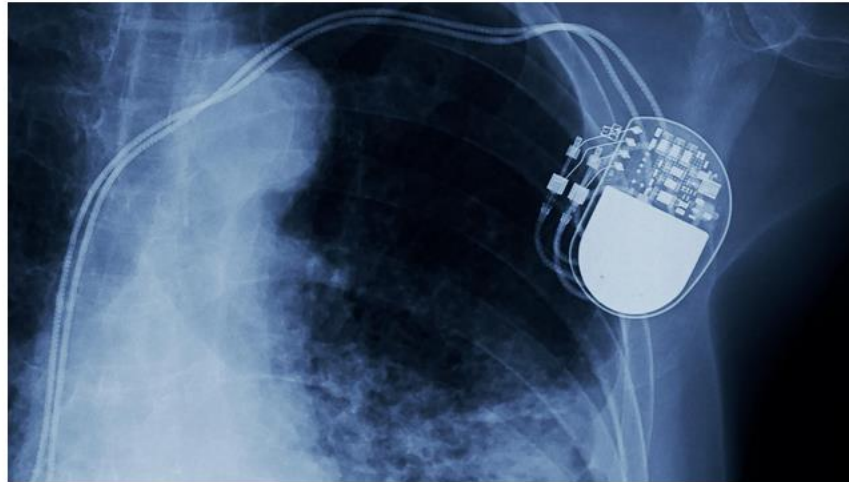


Image: [ChooChin](#)/Shutterstock

Patching has long been one of the most tedious chores for those who want to keep their electronic devices secure or up to date. Sometimes, patches require a restart, disrupting your workflow. Sometimes, patches screw up the software, making it unusable. These are just some of the reasons why users normally dread patching.

# Recent Hacks

x

←

→

↻

https://www.safegadget.com/139/hacked-internet-things-database


★

☰

Safegadget.com

Computer security, Smartphone Security, and Windows security

Contact



## Hacked Internet of Things Database


Last Update: August 24, 2018

SafeGadget

Internet of Things Scanner

Search ...

🔍

 Safegadget.com

# Recent Hacks: iKettles

October  
2015





# Recent Hacks: Ring door bell



January  
2016

# Recent Hacks: IP Camera

March  
2017





# Recent Hacks

July  
2015

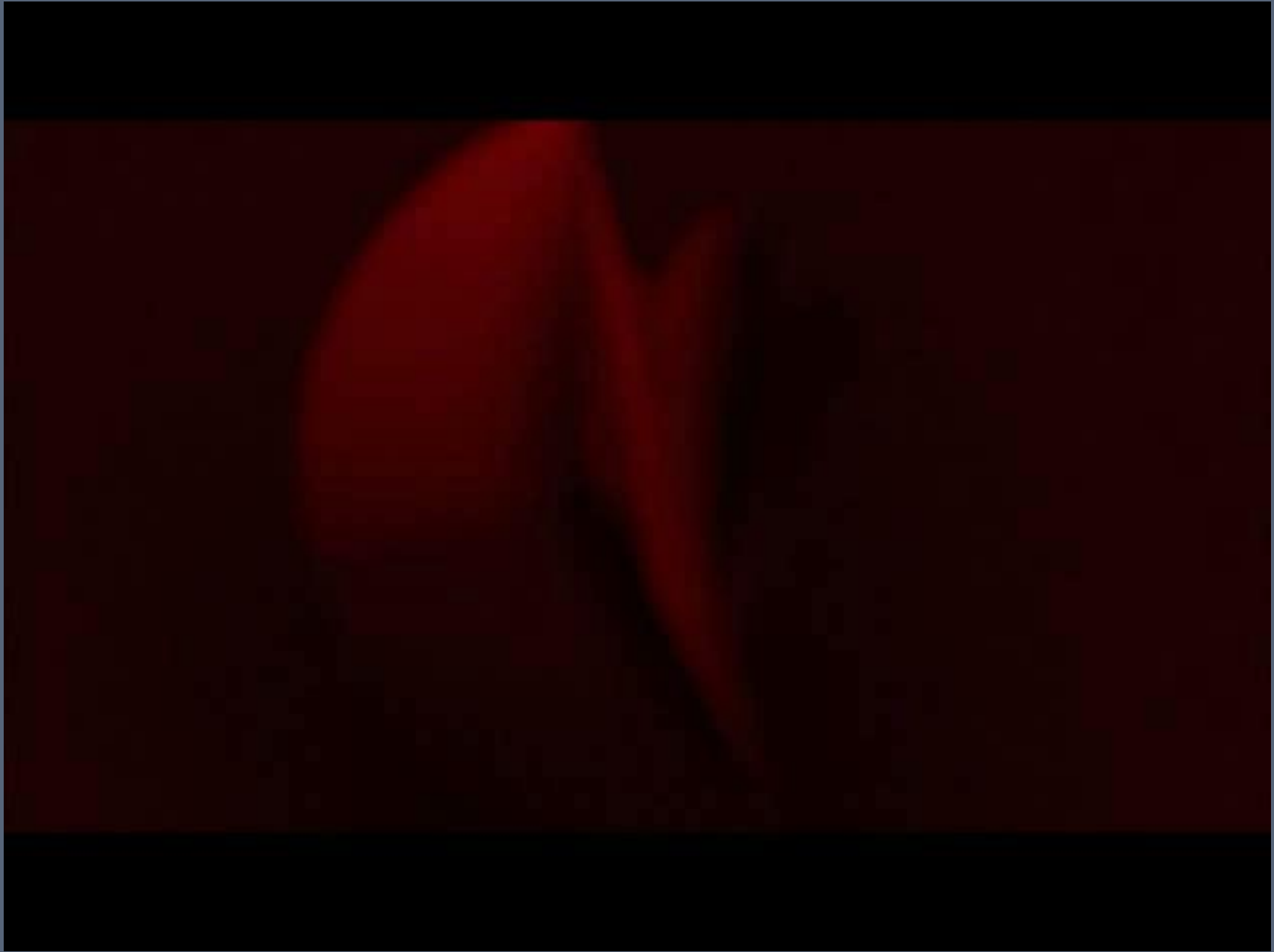
<https://www.safegadget.com/139/hacked-internet-things-database/>

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Hackers Remotely Kill a Jeep on the Highway—With Me i...





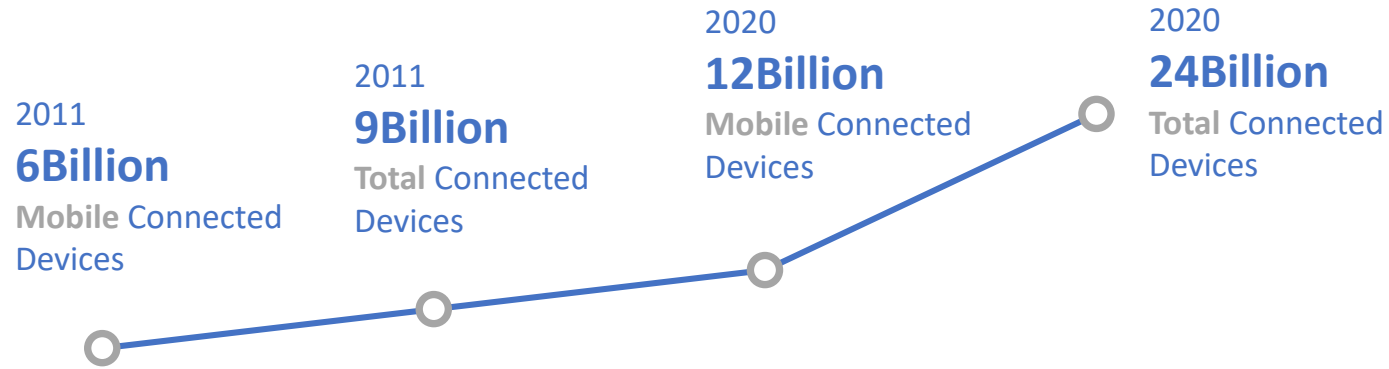
# Recent Hacks: E Skateboard

August  
2015





# Future of IoT: The Real Danger?



Revenue opportunity for connected devices in vertical sectors



Automotive  
\$202 Billion



Health  
\$69 Billion



Consumer electronics  
\$445 Billion



Utilities  
\$36 Billion

**\$1.2  
Trillion**

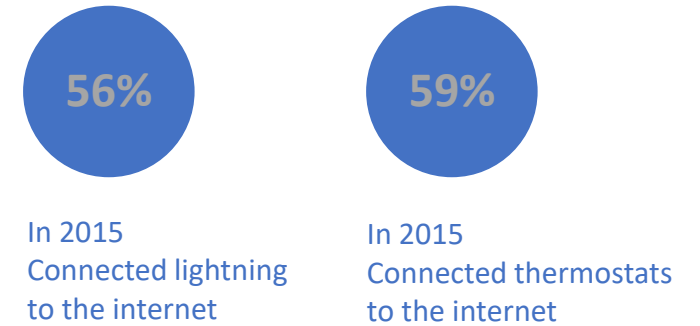
Revenue opportunity for  
Mobile Networks  
Operators in 2020

# Future of IoT: The Real Danger?

## Use of devices that are connected to the internet



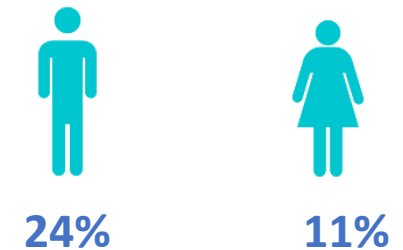
## Upcoming Technologies



## The Internet has changed life concerning



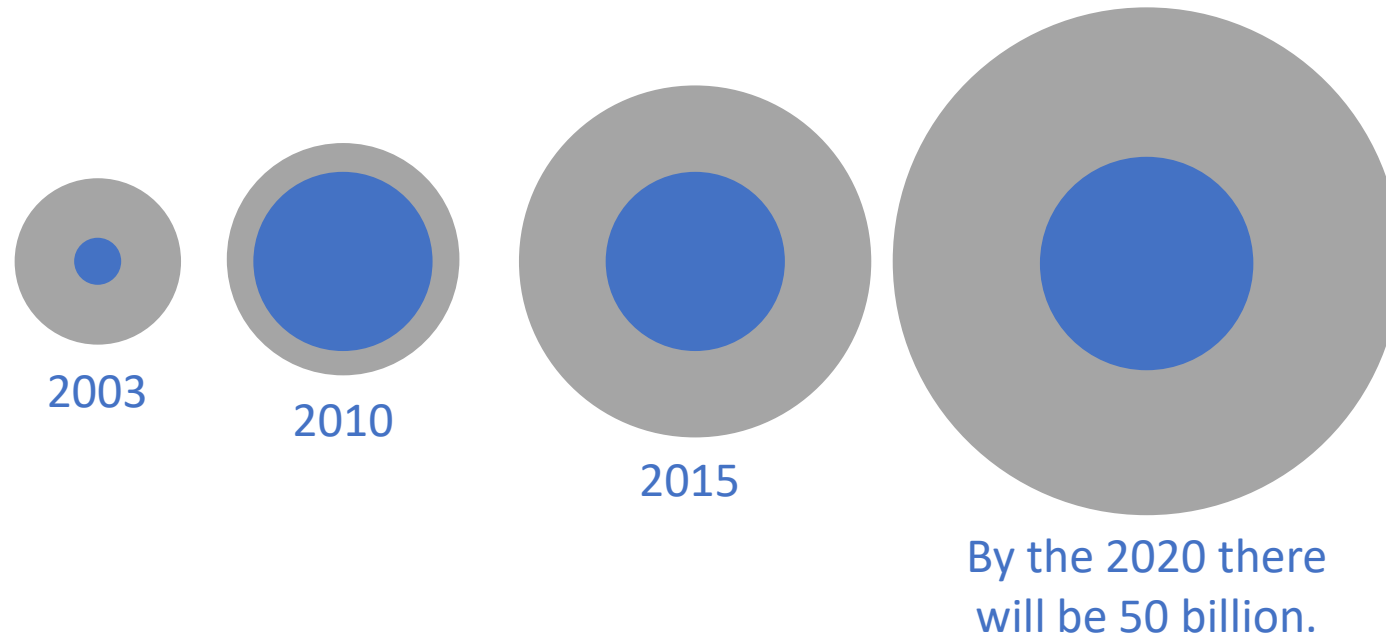
## Positive attitude towards Internet of Things



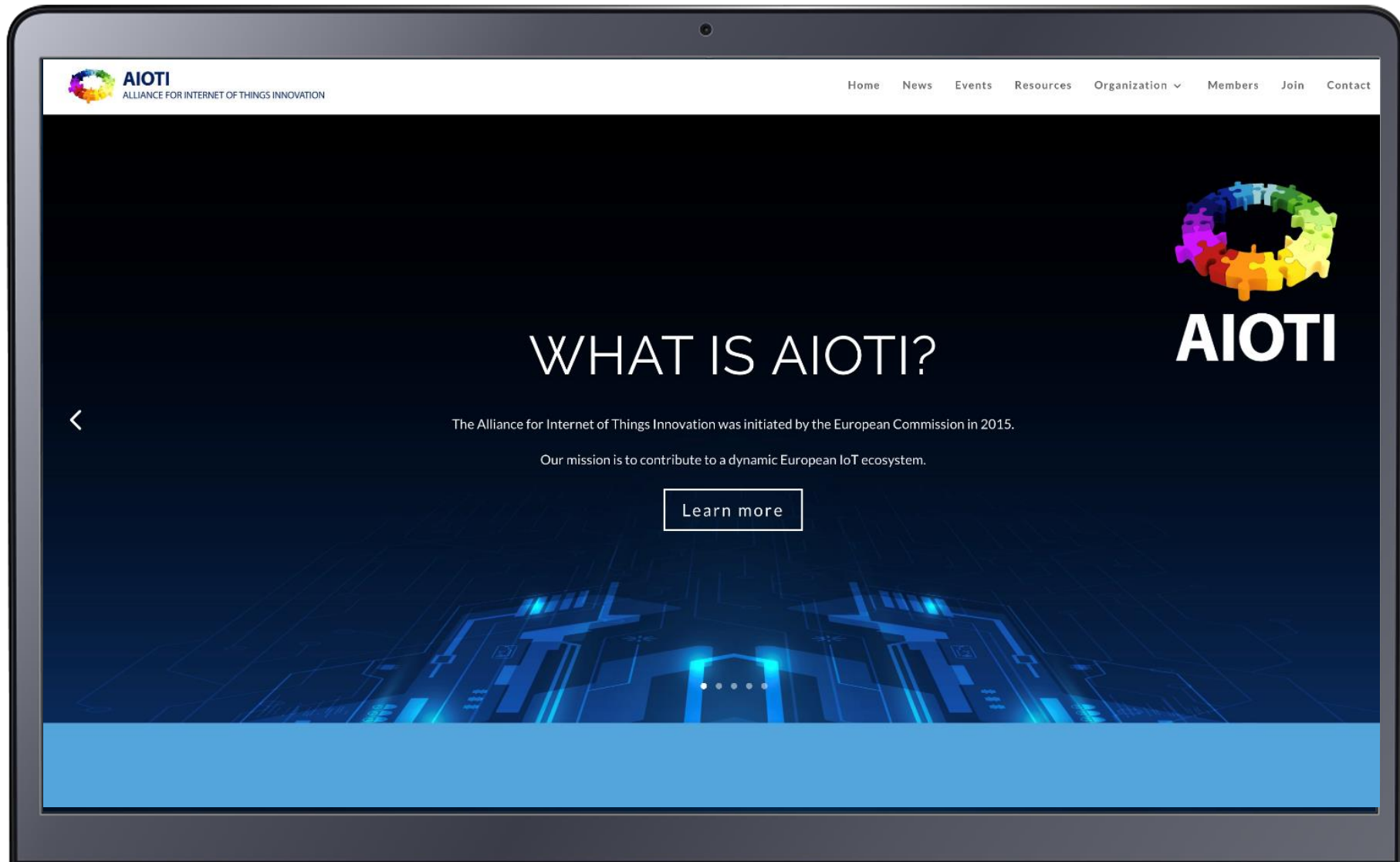


# Future of IoT: The Real Danger?

During 2008, the number of **things** connected to the Internet exceeded the number of **people** on earth.



# Defenses against IoT threats





# AIOTI

Alliance for Internet of Things  
Innovation

<https://aioti.eu/>

# Trends 2018: Critical infrastructure attacks on the rise



# Defenses



# Defenses

- Disconnect the network connection if the device is not using
- Avoid to connect the device on the unsafe network, such as public WiFi without password
- Set a strong password for accessing your WiFi network
- Change your WiFi password regularly
- Keep the device drivers/program up to date



# Thank you