EUROPEAN CYBER SECURITY MONTH

University of Luxembourg

How to survive in a digital world

Practical tips for everyone

Christian Hutter, Chief Information Security Officer

UNIVERSITÉ DU LUXEMBOURG

6,363 views | Sep 24, 2019, 05:00am

Androids And iP
Hacked With Jus
WhatsApp Click
Tibe
Ass

THE CONVERSATION

Academic rigour, journalistic flair

Arts · Culture Business · Economy Cities Education Environment · Energy Health · Medicine Politics · Society Science · Technology Brexit

22,406 views | Sep 17, 2019, 05:08am

Google Calendar Users Are One Click Away From Privacy Disaster

Davey Winder Senior Contributor

Cybersecurity

ng cybersecurity and privacy stories

19,120 views | Sep 3, 2019, 04:42pm

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor

Consumer Tech

I cover the human side of VR/AR, Blockchain, AI, Startups, & Media.

GDPR: LUX 7TH HIGHEST PROPORTION DATA BREACHES

NEWS • BUSINESS • 07.02.2019 • JESS BAULDRY

Luxembourg recorded the seventh-highest number of personal data breaches per capita from May 2018 to the end of January 2019.

According to a report by law firm DLA Piper, the grand duchy reported 200 data breaches in the eight months after the general data protection regulation (GDPR) entered into force.

While the total figure was low compared to larger European countries, when calculated per

Data Breach at Swindon College England

September 19, 2019

A cyber attack is reported to have resulted i
the information related to former and curren
Swindon College England. Highly placed source
where threat actors gained access to the last

EDITION: EU

ZDNet

MUST READ: Microsoft releases out-of-band security update to fix IE zero-day & Defender bug

Vulnerability in Microsoft CTF protocol goes back to Windows XP

Insecure CTF protocol allows hackers to hijack any Windows app, escape sandboxes, get admin rights.

By Catalin Cimpanu for Zero Day | August 13, 2019 -- 18:02 GMT (19:02 BST) | Topic: Security

Living in a dangerous world

- Why do things go south?
  - Broken by design
  - Badly configured systems
  - User making errors

Let's focus on what

YOU

can do today!

Perfect security is a myth

- You **are** a target and there is no such thing as perfect security
- It is not possible to stop a skilled attacker who wants your data
- So the question is **not if but only when** you will face a security incident

But…

There is still hope…

- Most attacks are not highly targeted but reach out to as many people as possible
- Take basic protection measures and make your digital home more secure



Secure your digital home

Protect your digital identity / data the same way you would protect your objects of value in the real life, e.g. in your home

- Think about the network as the floors connecting the rooms in your digital house
- The data you want to protect is stored in the rooms
- Depending on the sensitivity of the data you will have corresponding protection measures in place
- You might also have some valuable data outside your own house

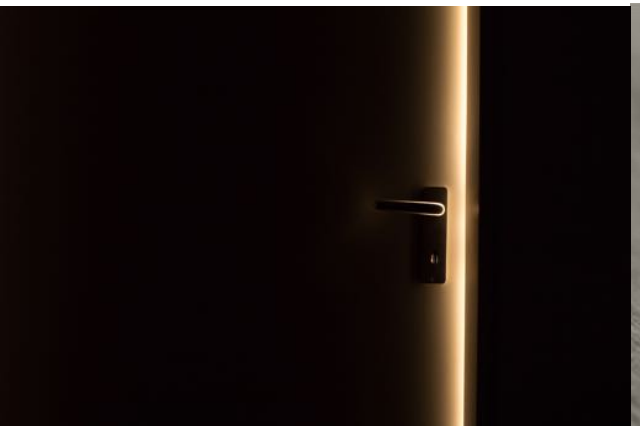
Would you leave your door or window open?

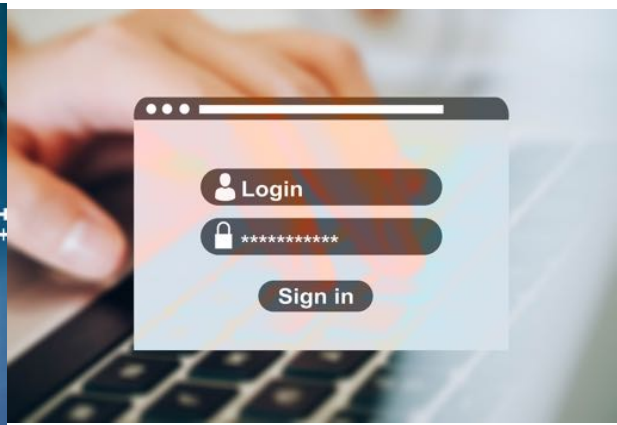
- An open door is an invitation for everyone to come in and invade your privacy; even an open window can be used to spy on you
- An unsecured / badly secured IT system allows and invites strangers from all over the word to try to check our your private data
- Close the doors and reduce or even stop the invasion of your privacy




Each door needs a good key

- Like keys, passwords open the door to access your data
- Strong passwords are like good locks with solid keys, more expensive but also more secure.
- One password for everything is a huge risk. Imagine one key for all your doors
- Mind the difference between single-sign-on (SSO) and password recycling
- A password manager is like a key ring, helping you to organise your keys as well as to find them back; they can also be used to generate strong passwords
- If available, multi factor authentication should be used to improve security (but choose a good one, SMS is NOT good)
- Biometric authentication can improve security



Regular maintenance is important

- Your home needs regular care taking to be in good shape, so do your IT systems
- When you see something not working or behaving in an unexpected way don't ignore it - act!
- When you see an alert, don't just click on "OK" or "Ignore"
- Regularly install system and application updates; don't ignore the prompts you get to do them

Have your defences ready

- You might have a fence to try to stop strangers at the boarder of your grounds
- Do the same for your personal data; make sure your firewall is active
- Install anti-virus / anti-malware and keep them up to date to have somebody watching who is coming in and stop bad / suspicious visitors
- Only use software from trusted sources
- Don’t use hacked / cracked software – these often include some special gifts
- If you don’t want to pay for your software, check out freeware, public domain or open source alternatives

Plan for Disaster recovery

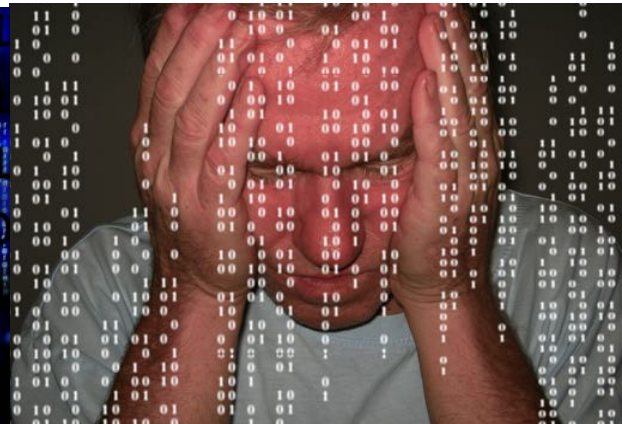
- Your house might be robbed, damaged, destroyed by flood, fire or other natural disasters, similarly your device might be lost, stolen, destroyed or simply malfunction
- Analyse which data you have and where it is stored
- Which of your data is already backed up?
- What is really important to you, what can you loose?
- Mind the gap between cloud storage, NAS and backup!
- Plenty of (free) tools available to help you!




Handling break-in / theft

- Be prepared to protect your data!
  - Enable device encryption on mobile and stationary devices
  - Powerful build-in (free) tools available for all major systems
    - Bitlocker for Windows
    - Filevault for Mac OS X
    - iPhone enables encryption when you set
- Even if a device is lost/stolen your data will be secure
- Try to wipe and lock stolen/lost devices
- After a break-in you might want to change your locks – same goes for your passwords
- Monitor your accounts for unusual behaviour





The house is hopefully secure, but what about interacting with others?

Email

- The same way one could put any sender name on an envelope, there is no way to be sure of the sender of an email
- Emails are still the most common attack vector
- Be suspicious when receiving an email from an unknown sender and try to verify the sender identity
- Try to avoid clicking on links in emails – except you are sure about the authenticity (e.g. confirmation mail after you did sign up for a new service)
- Want to test your skills? https://www.phishingbox.com/phishing-test

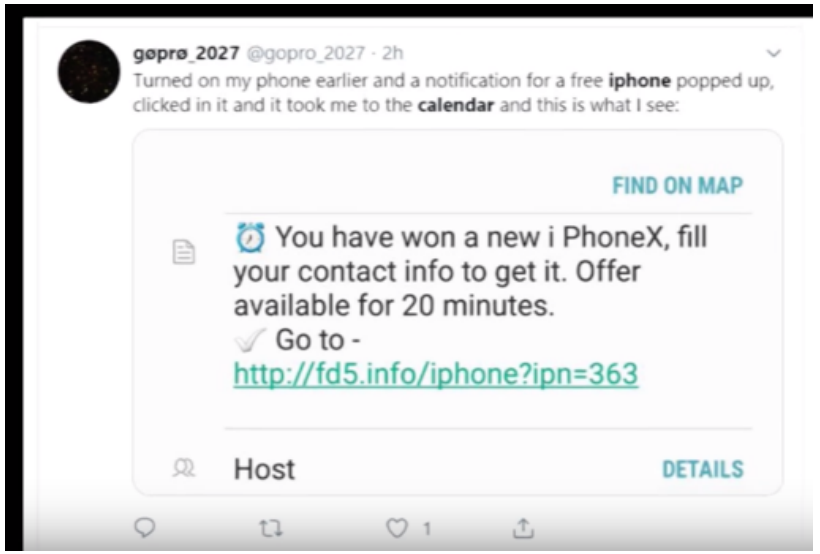

Social media

- Would you put a sign on in your window advertising that you are on holidays?
- Would you share intimate thoughts with complete strangers?
- The internet never forgets

- Think about what to share with whom
- Enable privacy settings
- Check e.g. the BEESECURE site for additional information



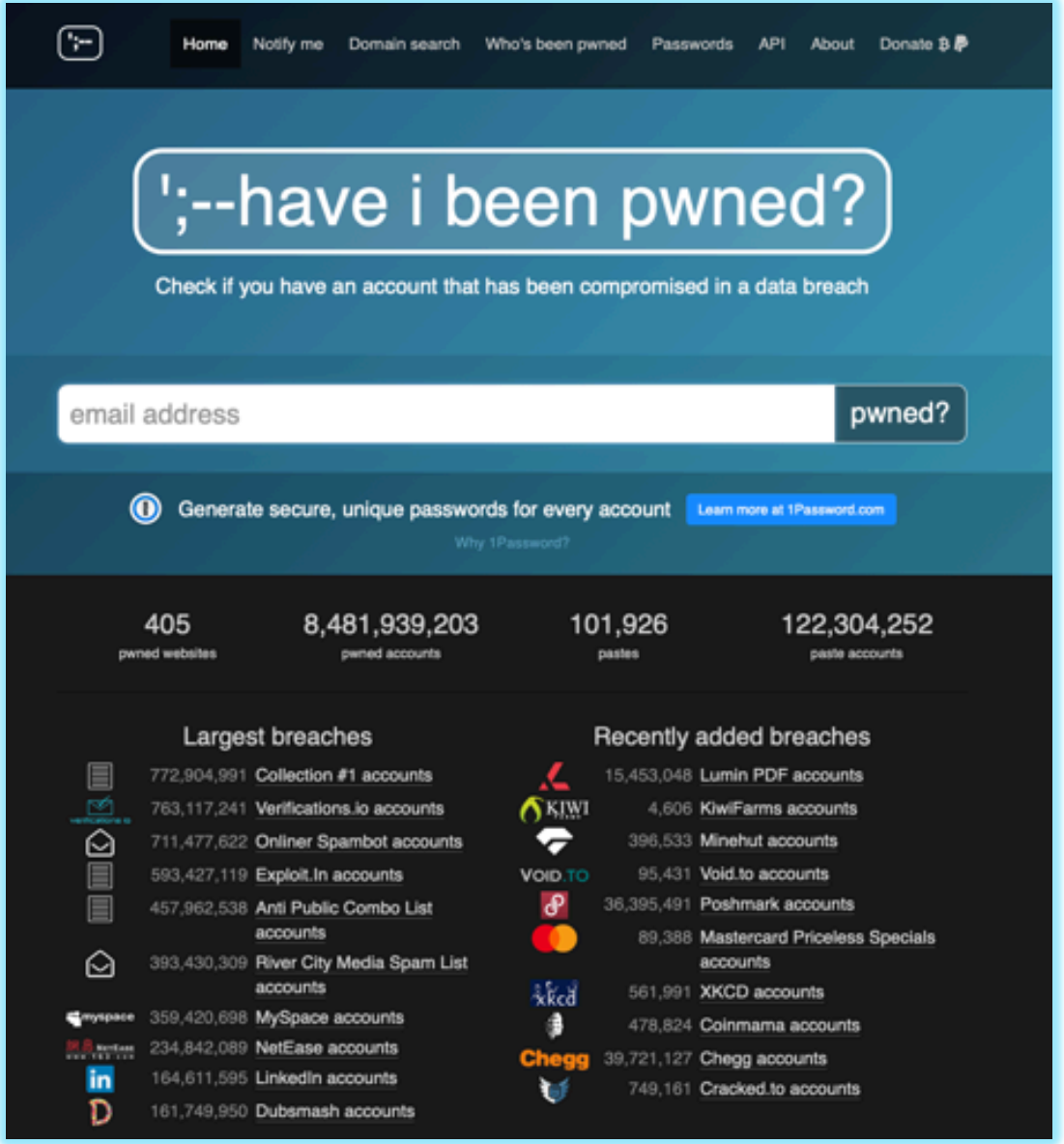
If it’s too good to be true, it is NOT true!



- Don’t be a zombie, use your brain!
- Would you trust a stranger ringing at your door?
- Nothing is for free, at least you will pay with your personal data
- Could be a door opener for a later attack
- Could be used to phish your credentials

Action Plan (1/2) - Secure your logins

- Find out if your email address is listed in a password breach https://haveibeenpwned.com
- Start using a password manager and use strong, unique passwords for each service
  - Plenty of free and paid choices, just google for something like “best password managers” and pick your favorite
- If available, enable MFA



Action Plan (2/2) - Start building up your defenses

- Get free advice from experts: https://www.securityplanner.org

Security is not child's play

Play

Questions?

THANK YOU
for your
ATTENTION!