

# Cybersecurity and Best Practices

Lorenzo Soligo - Ca' Foscari University of Venice  
Master's Degree in Digital Humanities - 2020

# Some rambling

- WordPress vulnerability database: <https://wpvulndb.com/>
- Twitter (IT): @raistolo @FiloSottile @evaristegal0is and many others
- Keep everything updated
- Keep backups
- Use password managers and impossible-to-remember passwords
- Use encryption wherever possible

# Why should I waste time updating stuff?



**evariste.gal**  **is** @evaristegal0is · 2h

Ho trovato tre XSS persistenti in tre plug-in WP con oltre 290.000 installazioni. Li segnalo e poi butto giù due righe sul perché bisogna stare molto attenti a chi si dà il privilegio di Author su WP :)

 Translate Tweet



3



4



26




# Still not updating, I only use safe apps

## **Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account**

Zoom's privacy policy isn't explicit about the data transfer to Facebook at all.

---

By Joseph Cox

Mar 26 2020, 2:00pm  Share  Tweet  Snap

## Zoom per iOS si aggiorna: ora non invia più dati a Facebook

30 Marzo 2020  72

# But I have an iPhone, Apple is the best at security

<https://googleprojectzero.blogspot.com/2020/01/remote-iphone-exploitation-part-1.html>

This research was mainly motivated by the following question: given only a remote memory corruption vulnerability, is it possible to achieve remote code execution on an iPhone without further vulnerabilities and without any form of user interaction? This blog post series shows that this is in fact possible.

# I don't like Windows 10, I'm sticking to Windows 7

[https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

"While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life."

# I hate runners! They are spreading the virus! Let's give geo-localization data to the government and have those killers arrested!

POLITICA

## Il fuorionda di Mattarella, "eh Giovanni, neanche io vado dal barbiere"



**Calogero Mandracchia** @CalogeroDebug · 9h

#INPSdown #INPS #600euro

Richiesta effettuata. Ad onor del vero, la richiesta era davvero disponibile dalla mezzanotte, riferendosi però all'orario del server dell'INPS che è 2 ore indietro al nostro:

```
> GET /PSRSVSCweb/welcome.do?idNav=WELCOME HTTP/1.1
> Host: serviziweb2.inps.it
> User-Agent: curl/7.58.0
> Accept: */*

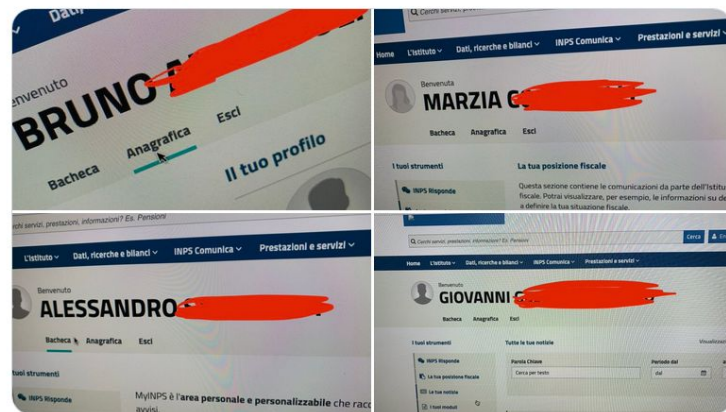
< HTTP/1.1 302 Found
< Date: Wed, 01 Apr 2020 00:35:23 GMT
< Location: https://serviziweb2.inps.it/PassiWeb/jsp/login.jsp?url=2FPSRSVSCweb%2Fwelcome.do%3FidNav%3DWELCOME&S=S
< Content-Length: 0
< Set-Cookie: JSESSIONID_SPOTELLOVIRTUALE=0000hq_Qmyrhx1vx_KF9SeP
< Expires: Thu, 01 Dec 1994 16:00:00 GMT
< Cache-Control: no-cache="set-cookie, set-cookie2"
< Content-Type: text/html
< Content-Language: it-IT
< Set-Cookie: BIGip_stat=1488214215;path=/;domain=.inps.it;
```



**Marco Rizzo** @Marco\_Rizzo · 1h

Il sito dell'INPS sta dando il meglio: adesso nella mia bacheca si alternano nomi di sconosciuti a seconda delle pagine dove clicco (e con tanto di codice fiscale).

Se è un #pescedaprile elaborato, i miei complimenti, altrimenti ho paura.



4



4



9



# Take-away

- Whenever you do something sensitive on a laptop or smartphone, beware of the risks and take precautions accordingly
- When non-technical people talk about tracking the population, "suspending" privacy laws, etc. remember *why* those laws exist in the first place
- Ask more of your representatives! Cybersecurity is as important as "classic" security: not having burglars in your home is nice, not seeing your personal data all over the internet because of some crappy developer at government agencies is even nicer.



# Food for thought

- [Yuval Noah Harari: the world after coronavirus](#)
- [Coronavirus: l'uso della tecnologia, il modello coreano e la tutela dei dati personali](#)
- [Terms of Service; Didn't Read. "I have read and agree to the Terms" is the biggest lie on the web.](#)