



# BIT

BARATTIERI INFORMATION TECHNOLOGY

---

# ITSec Quotidiana

La sicurezza informatica per tutti i giorni

A cura di Daniele Barattieri

# Programma

- ◆ **Intro**
- ◆ **I problemi dell'utente**
- ◆ **Tips & Tricks**
- ◆ **Contatti**

# Intro – Chi sono

- ◆ **Daniele**  
→ aka **MrMoDDoM**
- ◆ CyberSec Expert @ BIT
- ◆ MuHack co-founder
- ◆ Electronics enthusiast



# Ingegneria Sociale

- ◆ Generalmente, l'anello più debole è l'utente

## **Perché?**

- ◆ I computer si fidano dell'azione dell'utente

## **..e quindi?**

- ◆ La maggior parte degli attacchi al privato richiede l'interazione da parte dell'utente

# Ingegneria Sociale

- ◆ Generalmente, l'anello più debole è l'utente



Interazione da parte dell'utente

# Ingegneria Sociale

- ◆ Gli attacchi di **Social Engineering** puntano a far commettere degli errori all'utente
  - ▶ **Azioni ripetitive**
    - Login – Apertura di file – Click sui link
  - ▶ **Promesse**
    - Soldi – Risoluzione problemi – Se\*\*o

# La Password

- ◆ Deve essere:
  - ▶ **Lunga**
  - ▶ **Facile da ricordare**
- ◆ **NON** serve:
  - ▶ Che sia complessa
  - ▶ Cambiarla periodicamente
- ◆ Usare un password manager



KeeWeb

# La Password

**“In 20 anni di fatica, abbiamo con successo insegnato ad ognuno ad usare password che sono difficili da ricordare per gli umani, ma facili da indovinare per i computers.”**

**<https://xkcd.com/936/>**



# Two Factor Authentication

- ◆ I meccanismi di **2FA** ci proteggono dal furto delle credenziali
- ◆ Servono anche come doppio controllo
- ◆ Quasi ogni servizio “grosso” ha un sistema di 2FA  
→ **ATTIVATELO**

# Tips & Tricks

- ◆ **Come metto al sicuro i miei file?**
  - ▶ Backups → CloneZilla
  - ▶ Sistemi di cifratura → BitLocker o LUKS



<https://clonezilla.org/>

# Tips & Tricks

- ◆ **Vorresti davvero aprire quel link?**
  - ▶ Sandbox esterna
  - ▶ Analisi di comportamento
  - ▶ Indicatori



**<https://urlscan.io/>**

# Tips & Tricks

- ◆ **C'è un file sospetto?**

- ▶ Analisi multi-engine
- ▶ Sandbox per analisi del comportamento
- ▶ ... basta anche un solo risultato positivo!



**<https://www.virustotal.com>**

# Tips & Tricks

- ◆ **Com'è la mia situazione?**
  - ▶ Come – quando – cosa è stato rubato
  - ▶ Controllo incrociato di quali dati potrebbero essere stati resi pubblici

';--have i been pwned?

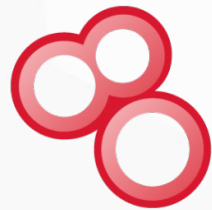
<https://haveibeenpwned.com/>

# Tips & Tricks

- ◆ **E per l'Intelligenza Artificiale?**
  - ▶ <https://isitai.com/> → foto & testo
  - ▶ <https://deepware.ai/> → video
- ◆ In generale, i contenuti generati da AI puntano a far leva sull'utente → **Social Engineering**

# Tips & Tricks - IT

- ♦ **Vuoi sapere come è messa la tua rete?**
  - Possibilità di utilizzare filtri
  - Ricerca anche per stringhe testuali
  - API e download dei risultati



**SHODAN**

**<https://www.shodan.io/>**

# Tips & Tricks - IT

- ◆ **E il tuo dominio dove porta?**
  - ▶ Informazioni circa gli shared hosts
  - ▶ Analisi dei record DNS globali

**<https://dnsdumpster.com/>**



# Disclaimer

- ♦ **La sicurezza informatica non è da sottovalutare!**  
È stato presentato un “**kit base**” per poter sopravvivere su internet, ma non è certamente esaustivo per difendersi da tutte le minacce...!

**Affidatevi ad un esperto in materia**

# Domande?



# Grazie!

- ◆ MrMoDDoM @ TG e Twitter
- ◆ <https://mrmoddom.github.io/>
- ◆ <https://muhack.org/>
- ◆ <https://www.barattieri.info/>



# BIT

BARATTIERI INFORMATION TECHNOLOGY

---



# Links

- ◆ <https://urlscan.io/>
- ◆ <https://www.virustotal.com>
- ◆ <https://www.shodan.io/>
- ◆ <https://dnsdumpster.com/>
- ◆ <https://isitai.com/>
- ◆ <https://deepware.ai/>