

Parte 3:

Suggerimenti pratici

Email

Password

PC = Smartphone = Tablet = ...

- **Tutto** quello che diremo vale per **ogni** tipologia di dispositivo

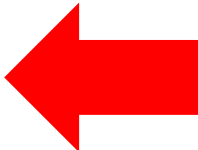
Difesa **IMPORTANTISSIMA**

- Aggiornamenti dei software (spesso) risolvono le vulnerabilità
- **Mantenere i software aggiornati**
- **Mai** disabilitare aggiornamenti automatici

Infatti

| SECURITY <u>NONEXPERTS'</u> TOP ONLINE SAFETY PRACTICES | VS | SECURITY <u>EXPERTS'</u> TOP ONLINE SAFETY PRACTICES |
|---|----|--|
| 1. USE ANTIVIRUS SOFTWARE | | 1. INSTALL SOFTWARE UPDATES |
| 2. USE STRONG PASSWORDS | | 2. USE UNIQUE PASSWORDS |
| 3. CHANGE PASSWORDS FREQUENTLY | | 3. USE TWO-FACTOR AUTHENTICATION |
| 4. ONLY VISIT WEBSITES THEY KNOW | | 4. USE STRONG PASSWORDS |
| 5. DON'T SHARE PERSONAL INFORMATION | | 5. USE A PASSWORD MANAGER |

Focus prossime slide

- Attacchi
 - Comuni
 - Semplici
 - Azioni Utente decisive per il successo 
- Impatto
 - Installazione malware
 - Consegnna username / password ad Attacker

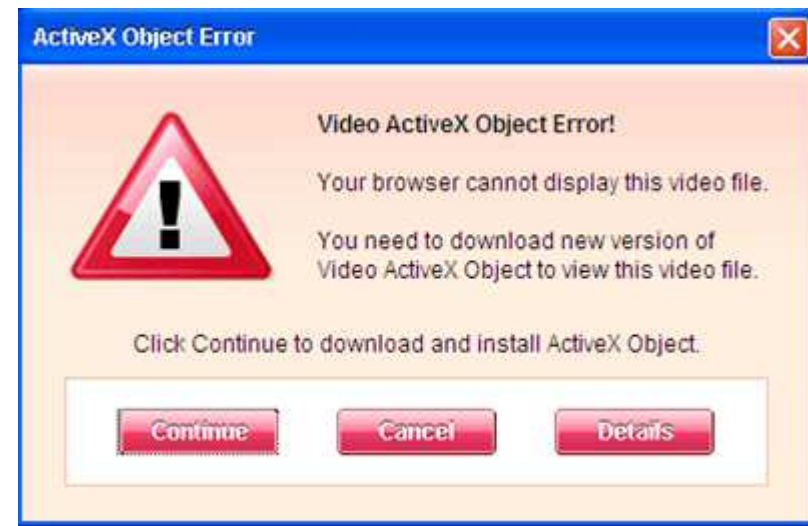
Social Engineering

- Ogni tecnica che **inganna** l'utente e lo convince ad eseguire azioni che provocano l'esecuzione di malware
- La difesa **non può** essere completamente tecnica
- Deve essere (anche) l'utente a difendersi

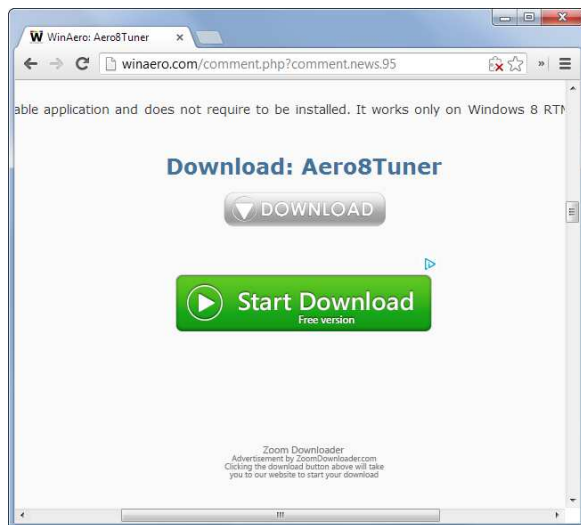
Social Engineering 1: Eseguire software che SEMBRA UTILE

- Attacker convince Utente ad eseguire software (**sembra utile** ma in realtà contiene malware)
- Metodo comunissimo (anche su smartphone):
Pagina web propone eseguire software

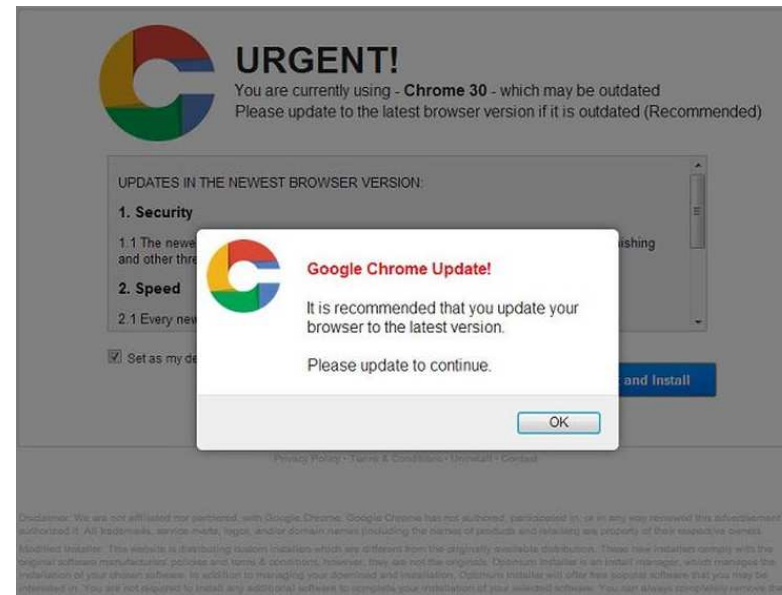
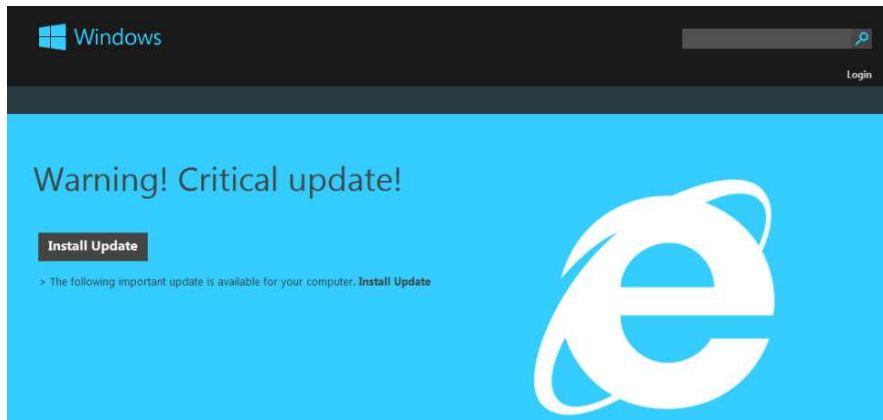
Mai INSTALLARE sw su proposta web (“missing codec”)



Mai INSTALLARE sw su proposta web (“software update”)



Mai INSTALLARE sw su proposta web (“software update”)



Mai ESEGUIRE sw su proposta web ("antivirus scan")



Come comportarsi

- Ogni proposta di install / update **inattesa** deve essere ignorata
- **Chiudere** la pagina web ed infischiarvene della proposta
- Se proprio desidero installare software:
 - Cercare su Google + Click sul risultato
 - Maggiore garanzia di arrivare su pagina web legittima

Lezione Importantissima

- ❑ **UN** click può essere sufficiente per consegnare il proprio dispositivo (ed i dati) ad un attaccante
- ❑ Ripeto: **UN** click
- ❑ Non si deve smettere di clickare
- ❑ Ma prima di clickare si deve **riflettere**

Social Engineering 2 (I): Eseguire software **SENZA SAPERLO**

- **Attacker convince Utente a vedere file / pagina**
(visione provoca esecuzione malware)

- Metodo **comunissimo:**
Email ricevuti

Social Engineering 2 (II): Eseguire software **SENZA SAPERLO**

- Attacker convince Utente a **vedere file/pagina**
(visione provoca esecuzione malware)
- **Click su allegato**
(vulnerabilità del lettore allegati)
- **Click su link**
(vulnerabilità del browser)
- UN click = Game over

Un "classico"



**Sembra una
cartella
esattoriale ma è
un virus: già
colpiti la Camera,
gli Interni e
Trenitalia**



Lo hanno creato su misura per le aziende italiane e viene distribuito come una mail che sembra provenire dal ministero delle Finanze. TaxOlolo ha colpito più di 80 compagnie ed enti. Tra loro Aci, Fineco, Autostrade e i comuni di Brescia e Bologna. L'attacco è partito da un server inglese pagato probabilmente in bitcoin

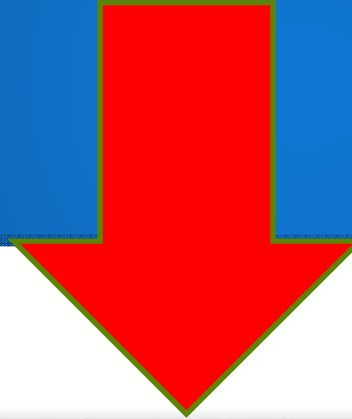
Perché la email è un metodo efficace?

- Molto semplice:
 1. Falsificare **mittente**
 2. Replicare **aspetto email** di quel mittente
 3. Ingannare sul **contenuto** di allegati / link

Dato di fatto 1: Falsificare Mittente


- ❑ Chiunque può inviarti con poco sforzo un email il cui mittente è:
 - ❑ Facebook
 - ❑ Equitalia
 - ❑ Un alto dirigente di un ente di ricerca
 - ❑ Il tuo migliore amico
 - ❑ Un tuo familiare
 - ❑ ...

Falso



From: Facebook [mailto:notification@facebook.com]
Sent: 17 July 2012 15:38
To: [\[redacted\]](#)
Subject: Christine McLain Gibbs tagged a photo of you on Facebook

facebook

 [Christine McLain Gibbs](#) added a photo of you.

[See Photo](#) [Go to Notifications](#)

If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).
Facebook, Inc. Attention: Department 415 P.O. Box 10005 Palo Alto CA 94303

Mi vuole Zidane...



COMPOSE

Inbox (1)
Sent Mail
Spam (377)
Automator
FwdAurora
RTM-Delega
RTM-Home
RTM-Work
Wait-Delega

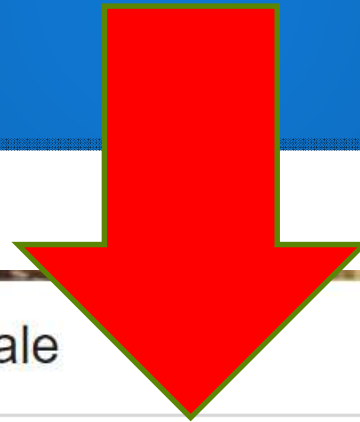
Manca un

 **Zizou** zinedine.zidane@realmadrid.es via units.it
to bartoli.alberto

Sergio Ramos ga ma a un pie, te rivi vegnir ti?

Sappime dir.
Ciau

Ahem...



COMPOSE

Inbox (1)
Sent Mail
Spam (377)
Automator
FwdAurora
RTM-Delega
RTM-Home
RTM-Work
Wait-Delega
Wait-Home
Wait-Work
Projects

Ospedale



Rettore@units.it

to Bartoli

Ci mancava solo questa...ma non hanno altro da fare???

[L'Ospedale Militare: Truffa o Superficialit  ?](#)

Il Piccolo, Gioved  14 Aprile 2016

Sent from my Windows Phone - apologize for misspelling.

Dato di fatto 2: Replicare Aspetto

- ❑ Chiunque può inviarti con poco sforzo un email il cui mittente è falso
- ❑ Chiunque può replicare con poco sforzo i **contenuti** tipici di quel mittente

Falso (Equitalia)

Agente della Riscossione
Equitalia S.p.A.
Via Cristoforo Colombo 142 - 481276 - Roma

Art. 4276 D.P.R. 07/03/1942, n. 691 e successive modifiche - Art. 4276 D.P.R.
02/07/1942, n. 5276, Art. 190 c.p.c.

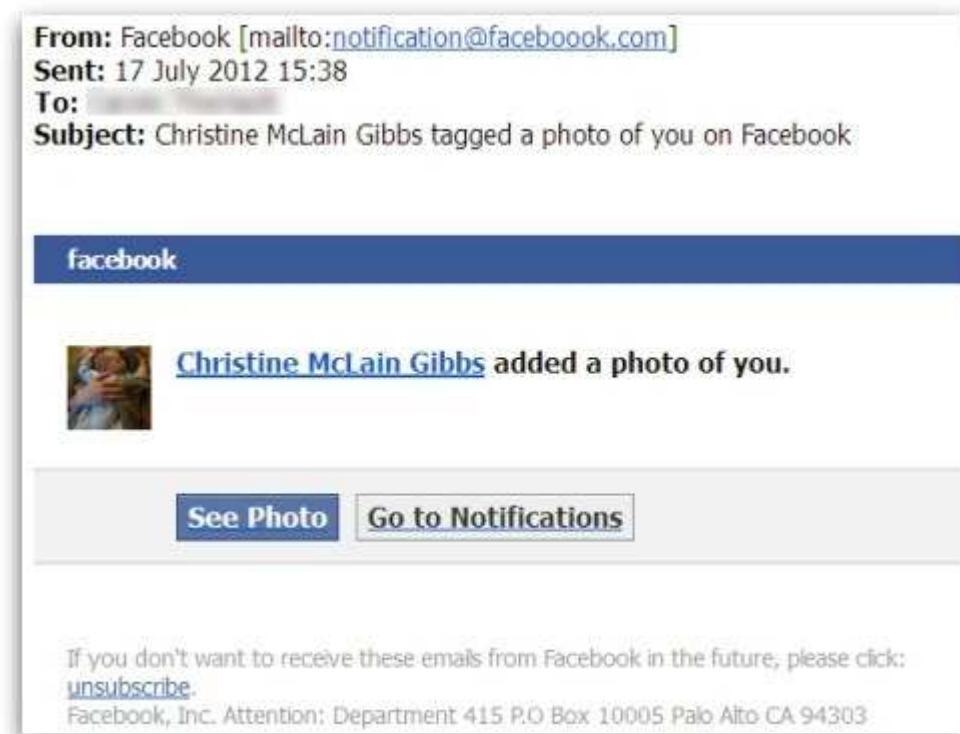
Gentile 

Il suindicato Agente della Riscossione avvisa, ai sensi delle intestate disposizioni di legge ,
di aver depositato in data odierna, nella Cassa Comunale del Comune il seguente avviso di
pagamento "**Documento n.006943470915**" del 09/15/2016 , composto da 5 pagina/e
di elenchi contribuenti a nr. 9 atti.

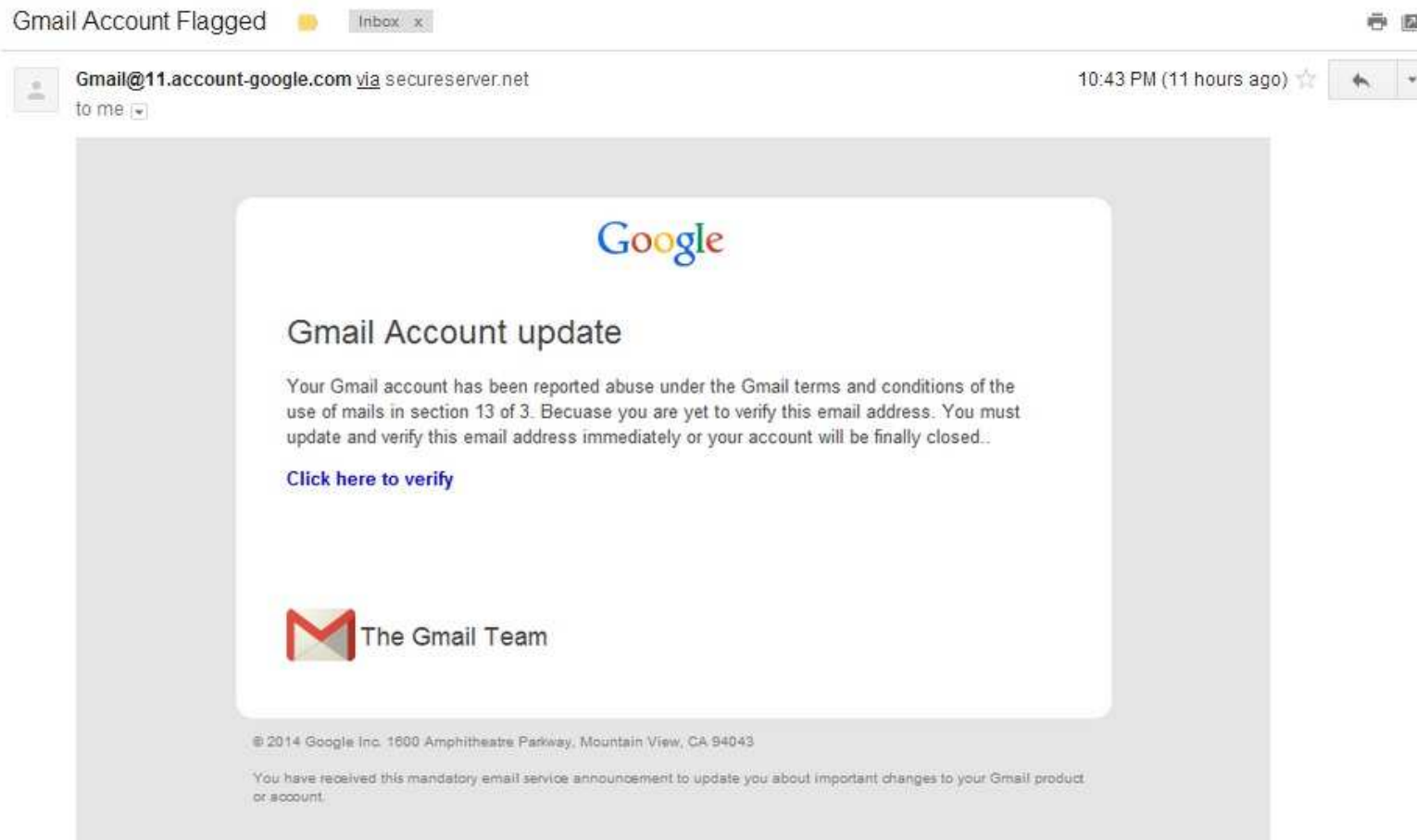
[Si prega di scaricare la fattura](#)

Equitalia S.p.A. C.F. P.I. 54276684276

Falso... (Facebook)



Falso... (Google)



Dato di fatto 3: Ingannare sul contenuto: ALLEGATI

- ❑ Nome fa pensare ad un contenuto
- ❑ **Contenuto reale** completamente diverso

- ❑ verbale-cda-21-Nov.pdf
- ❑ accertamento-fiscale.pdf
- ❑ Commissione-magistrale-24 Gen.docx
- ❑ . . .

Dato di fatto 3: Ingannare sul contenuto: LINK

- ❑ **Testo** fa pensare ad un sito web
- ❑ Contenuto reale su sito web **completamente diverso**

Ci mancava anche questa!!!

[Il Piccolo – La truffa dell’Ospedale Militare](#)

Su quale sito vado se faccio click?

[ANVUR – Nuovi requisiti accreditamento](#)

[Regione FVG – Aggiornati i bandi POR](#)

[Circolare sulla retribuzione degli straordinari](#)

[Solo 100 Biglietti gratis, affrettati su Ryanair!!!](#)

Conseguenza

- ❑ **Ogni email ricevuto** deve essere trattato con precauzione
- ❑ **Mai** clickare su link / allegato **impulsivamente**
- ❑ Ripeto: **MAI**
 - ❑ **Un click** può essere sufficiente per installare malware

Email ricevuti: Come comportarsi

- ❑ Quando ci sono una o più di queste condizioni:
 1. Email **inatteso**
 2. Contenuto che **ci stimola moltissimo**
(in positivo o in negativo)
 3. **Poco testo**

- ❑ **NON clickare impulsivamente: pensarci molto bene**
 - ❑ Provare a chiedere a qualche collega
 - ❑ Provare a contattare il mittente per via **diversa** da email

Importantissimo

- ❑ **Mittente noto, affidabile**

- ❑ **Non** deve essere utilizzato per decidere
- ❑ (Spesso) semplice da falsificare

- ❑ Suggerimenti su Internet discutibili
 - *"Non aprire allegati inviati da mittenti sconosciuti..."*

Osservazione utile 1

- ❑ Quando ci sono una o più di queste condizioni:
 1. Email **inatteso**
 2. ...
 3. ...

- ❑ Email ricevuti "**in una conversazione**" sono molto meno a rischio
 - ❑ Il vero rischio è sul **primo** email

- ❑ Più mi sorprende e più devo stare attento

Osservazione utile 2

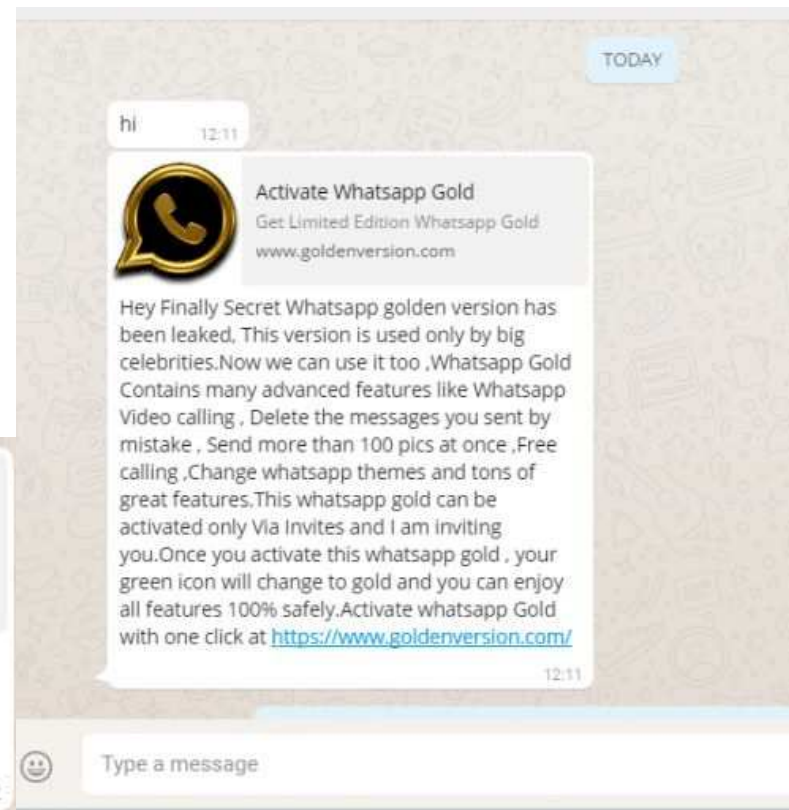
- ❑ Se arriva da un **sito in cui abbiamo un account**
- ❑ Allora andare sul sito **direttamente** e fare login
(**SENZA seguire link nell'email**)
- ❑ La notifica ci sarà di sicuro
- ❑ Se non c'è allora è un falso
- ❑ Non c'è il rischio di perdere notifiche importanti

Osservazione utile 3

- ❑ Se contiene un link su un certo argomento
- ❑ Allora andare sul sito **direttamente**
(**SENZA seguire link nell'email**)
- ❑ L'argomento ci sarà di sicuro...
...magari dopo qualche ora
- ❑ Se non c'è allora è un falso
- ❑ Non c'è il rischio di perdere notifiche importanti

Whatsapp / SMS: Stessi problemi (meno uno)

- ~~1. Falsificare mittente~~
2. Replicare aspetto
3. Ingannare contenuti

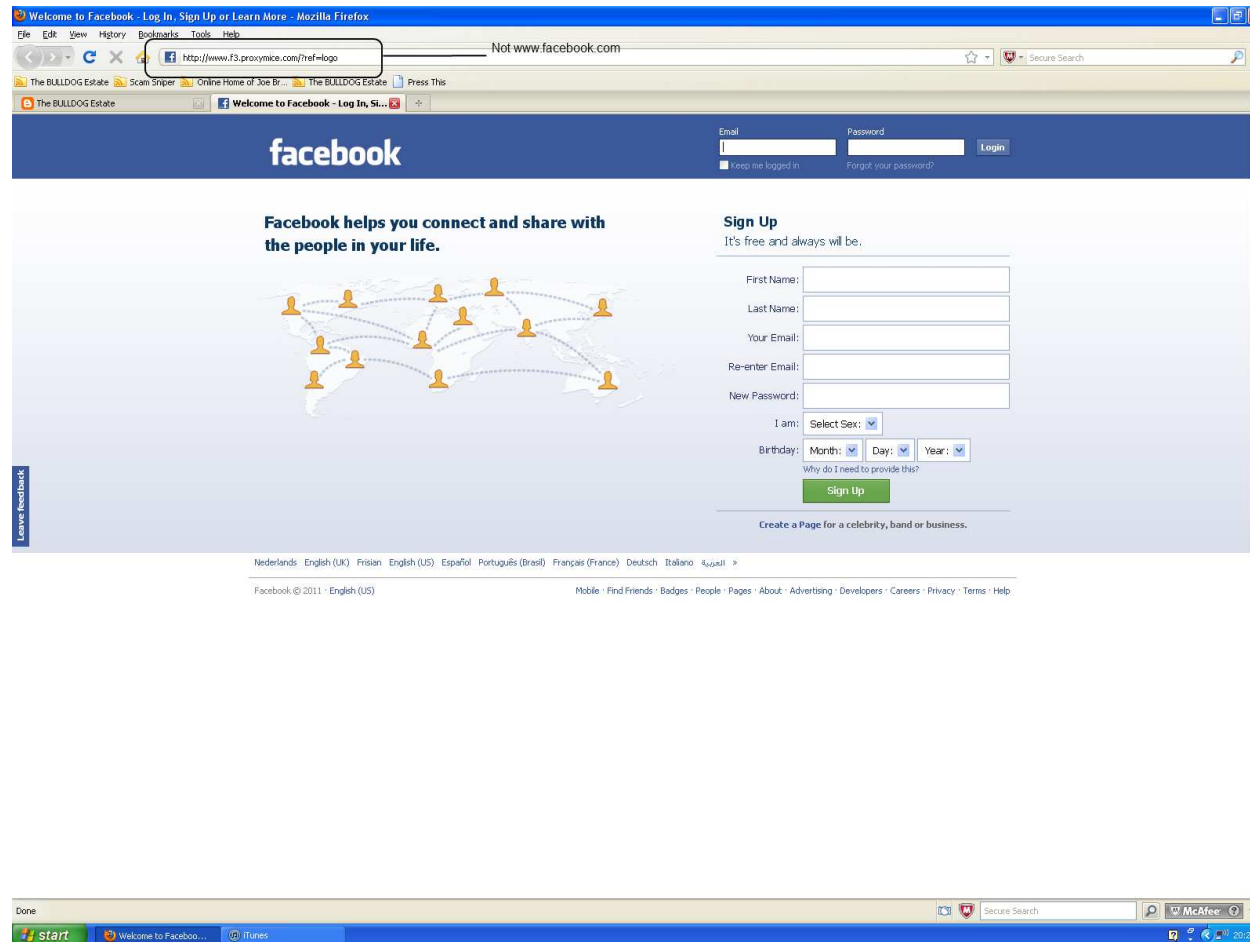


Social Engineering 3: Dare la password all'attaccante

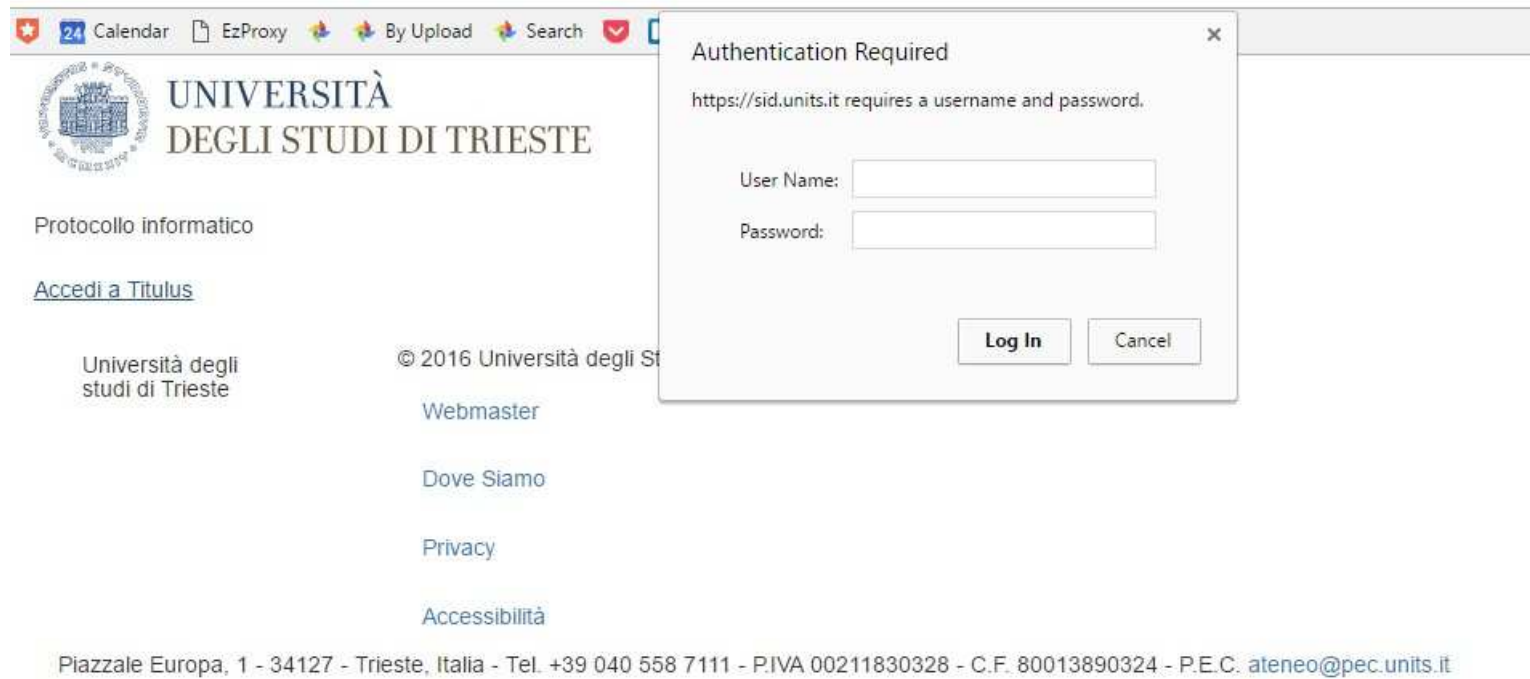
- Attacker convince Utente a vedere pagina web "importante" ma **falsa**
- Utente si fida ed **inserisce informazioni** (phishing)

- Metodo comunissimo:
Email ricevuti

Vera o falsa?



Vera o falsa?



The image shows a screenshot of a web browser displaying the website of the University of Trieste. The browser's address bar shows the URL `https://sid.units.it`. The website header includes the university's logo and the text "UNIVERSITÀ DEGLI STUDI DI TRIESTE". Below the header, there are links for "Protocollo informatico" and "Accedi a Titulus". The footer contains contact information: "Piazzale Europa, 1 - 34127 - Trieste, Italia - Tel. +39 040 558 7111 - P.IVA 00211830328 - C.F. 80013890324 - P.E.C. ateneo@pec.units.it".

An "Authentication Required" dialog box is overlaid on the right side of the browser window. The dialog box contains the following text and fields:

Authentication Required
`https://sid.units.it` requires a username and password.

User Name:

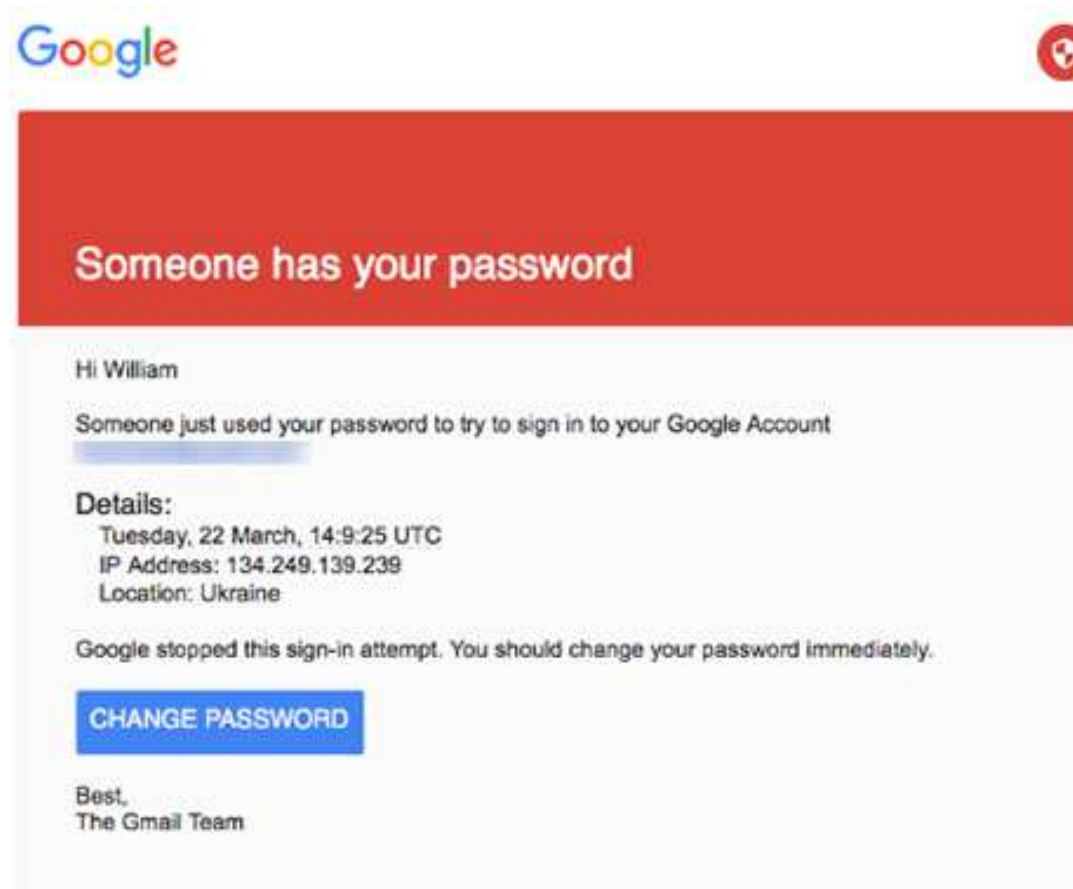
Password:

Log In Cancel

Perché il phishing (siti web falsi) è un metodo efficace?

- ❑ Chiunque può replicare con poco sforzo l'aspetto di **(qualche pagina di) un sito web**
- ❑ ...chiunque può creare una pagina web che **sembri**:
 - ❑ Gestionale di lavoro
 - ❑ Unicredit
 - ❑ Facebook
 - ❑ ...

Come sono arrivati alle email di Hillary Clinton



You received this mandatory email service announcement to update you about important changes to your Google product or account.

Difficile riconoscere pagina web legittima

- ❑ Indirizzo sito web falso sarà **diverso**
da indirizzo sito web vero...
- ❑ ...ma accorgersene è **complicato**

- ❑ Talvolta anche per un esperto

Vero o falso?

`http://promo.net/Ryanair`

`http://zara.offerteestate.com`

`https://offerte-decathlon.net`

`https://help-facebook.hosting.it`

Pagine di login: Come comportarsi

- ❑ Mai inserire credenziali in pagine web a cui si è arrivati con **click su email**
- ❑ **Mai**
- ❑ Arrivarci **sempre per altra via** (SEMPRE)
 - ❑ Google
 - ❑ Scrittura con auto-completamento
 - ❑ Bookmark
 - ❑ ...

Attacchi via email: Metodo frequentissimo

- Email **generico** inviato a **tantissimi** bersagli
 - Stesso email per tutti
- Costo attacco: bassissimo
- Opportunità guadagno: una per bersaglio

Metodo meno frequente (ma pericolosissimo)

- Mail **specifico** creato appositamente per **un** particolare bersaglio
 - Un email diverso per ognuno
- Difficilissimo da rilevare
- **Estremamente efficace**
- Spear phishing
<http://reti2.blogspot.it/search?q=spear>

Attenzione!

- Costo attacco: molto alto
- Opportunità guadagno: solo una

- Diretto a bersagli di alto valore
 - **Dirigenti**
 - **Segreterie dei dirigenti**
 - **Amministratori di sistema**

 - **Devono essere ancora più vigili degli altri**

Ahem...

BECCATO!!!

Aggiornato 15 Apr 2016

Segnalazione SPAM 

BECCATO!!!

Il mittente del mail era falso. Il link contenuto nel mail era falso.

Premere su quel link è stato un gesto incauto. Se il mail fosse stato inviato da un hacker, è molto probabile che adesso il suo PC o smartphone sarebbe entrato nel pieno controllo dell'hacker (*ad esempio, avrebbe potuto inviare all'hacker tutto ciò che scrive su tastiera, comprese username e password; avrebbe potuto crittare il disco e chiedere un riscatto per decrittarlo; avrebbe potuto eseguire qualsiasi programma a sua insaputa; etc etc*).

Ovviamente, in quel caso non sarebbe comparsa questa pagina: sarebbe comparsa una pagina di errore e l'attacco sarebbe rimasto completamente nascosto.

*PS Non ho avuto tempo di preparare un sistema automatico per avvisarmi dell'esito dell'esperimento; le sarei grato se mi inviaste un mail direttamente:
bartoli.alberto@univ.trieste.it*

<http://bartoli.inginf.units.it>

Ricapitolando

- Attacchi basati su **inganno**
 - **Email** metodo efficacissimo
- **Mai clickare impulsivamente su link/allegati email**
 - **Trattare email inattesi e stimolanti con sospetto**
 - **Valutare conferme per via diversa da email**
- **Mai “credere” a pagine a cui si arriva via email / SMS / Whatsapp**
 - **Arrivare a quelle pagine per via diretta**

Password: Perché è importante

- Quasi sempre **sufficiente** per eseguire azioni di cui **tu apparirai responsabile**
- **Semplifica** moltissimo il superamento di eventuali difese aggiuntive (SMS o smartcard)

**E' un problema reale
anche per noi?**

OMISSIS

Password: Come può essere trafugata (I)

1. Malware sul dispositivo dove si inserisce
2. Phishing
3. ...
4. ...

Come comportarsi

1. Malware sul dispositivo dove si inserisce
 - **Mai inserirla in dispositivi non nostri**
 - Caso comune: Postazioni pubbliche
 - Se proprio devo farlo, cambiarla il prima possibile (usando il **proprio** dispositivo)
2. Phishing
 - Già visto

Password: Come può essere trafugata (II)

1. Malware sul proprio dispositivo
2. Phishing
3. Per tentativi
4. Furto sul server

Furto sul server: Frequentissimo

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

pwned?

233

pwned websites

4,729,225,727

pwned accounts



164,611,595 LinkedIn accounts



152,445,165 Adobe accounts

La mia è stata rubata 6 o 7 volte

bartoli.alberto@univ.trieste.it

pwned?

Oh no — pwned!

Pwned on 3 breached sites and found no pastes (subscribe to search sensitive breaches)



Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

Furto sul server: Frequentissimo

Milioni di email e password rubate (anche in Italia) sono in un gigantesco archivio nel deep web



La nuova minaccia si chiama Anti Public, un data leak da 17 Giga. Più di 450 milioni di indirizzi mail da tutto il mondo, centinaia di migliaia di account a rischio tra aziende, polizia, militari, infrastrutture critiche e istituzioni europee. Possono essere usati per prendere il controllo dei server delle organizzazioni a cui sono state rubate

26 maggio 2017



Furto sul server: Frequentissimo

**Online 1 miliardo
e 400 milioni di
email e password.
E l'hacker chiede
donazioni in
bitcoin**



L'hanno chiamata Breach Compilation: raccoglie 252 leak precedenti ed è aggiornata alla fine di novembre 2017. La password usata per posta e social da 9 milioni di account è sempre la stessa: "password"

12 dicembre 2017



<http://bartoli.inginf.units.it>

126

Password: Come dobbiamo SCEGLIERLA

1. Malware sul proprio dispositivo
2. Phishing
Scelta influente
3. Per tentativi
"Sufficientemente complicata"
4. Furto sul server
Diversa per ogni sito

Nota bene

1. "Sufficientemente complicata"
2. Diversa per ogni sito

- **2 è molto più importante di 1**

Infatti

| SECURITY <u>NONEXPERTS'</u> TOP ONLINE SAFETY PRACTICES | VS | SECURITY <u>EXPERTS'</u> TOP ONLINE SAFETY PRACTICES |
|---|----|--|
| 1. USE ANTIVIRUS SOFTWARE | | 1. INSTALL SOFTWARE UPDATES |
| 2. USE STRONG PASSWORDS | | 2. USE UNIQUE PASSWORDS |
| 3. CHANGE PASSWORDS FREQUENTLY | | 3. USE TWO-FACTOR AUTHENTICATION |
| 4. ONLY VISIT WEBSITES THEY KNOW | | 4. USE STRONG PASSWORDS |
| 5. DON'T SHARE PERSONAL INFORMATION | | 5. USE A PASSWORD MANAGER |

In pratica?

1. Suggestimenti terra-terra
 - **Non ottimali**
 - Molto migliori di quanto si fa di solito
 - Applicazione **molto facile**
(quindi niente scuse)
2. Cammino verso la santità
 - Il meglio della tecnologia odierna
 - Un pò più complicato

"Sufficientemente complicata" (I)

- Lunga almeno **10 caratteri** (12 è meglio)
- Facile da **ricordare**
 - Niente caratteri speciali o cifre in posizioni strane
 - Se necessari, unico scopo è ricordarli (non è renderla più complicata)
- Non associabile a noi da **chi ci conosce**
 - Figli, compagni, date, scuole, indirizzi, cani/gatti...

"Sufficientemente complicata" (II)

- Lunga almeno 10/12 caratteri
- Facile da ricordare
- Non associabile a noi da chi ci conosce
- Non legata a **concetti** quali:
 - Luogo o ambiente di lavoro
 - Attività gradevoli
(sport, viaggi, turismo, sesso, ...)
 - Sito in cui la uso
(nome del sito, nome utente, ...)

"Sufficientemente complicata": Suggerimento

- Due / Tre sostantivi
- Completamente scorrelati tra loro
- Lontani da noi / concetti da evitare

polentapistone
corallocontrattoago
suolaplatanocamino

suolaplatano **lopta**

Diversa per ogni sito: Come ricordare? (I)

- Inventati un metodo di **raggruppamento** siti
- Usa una password **diversa** per ogni gruppo

1. importanti `suolapistone`
2. banche `corallocontratto`
3. non interessanti `pilastroippodromo`

- Univoca almeno nei gruppi interessanti

`suolapistoneunits`
`suolapistonefacebook`
`corallocontrattopaypal`
`corallocontrattobanca`

Diversa per ogni sito: Come ricordare? (II)

- Univoca almeno nei gruppi interessanti
suolapistoneunits
suolapistonefacebook
corallocontrattopaypal
corallocontrattobanca
- Certamente non ottimale
- Certamente molto migliore di quanto si fa di solito

Ma non le dovrei cambiare spesso?

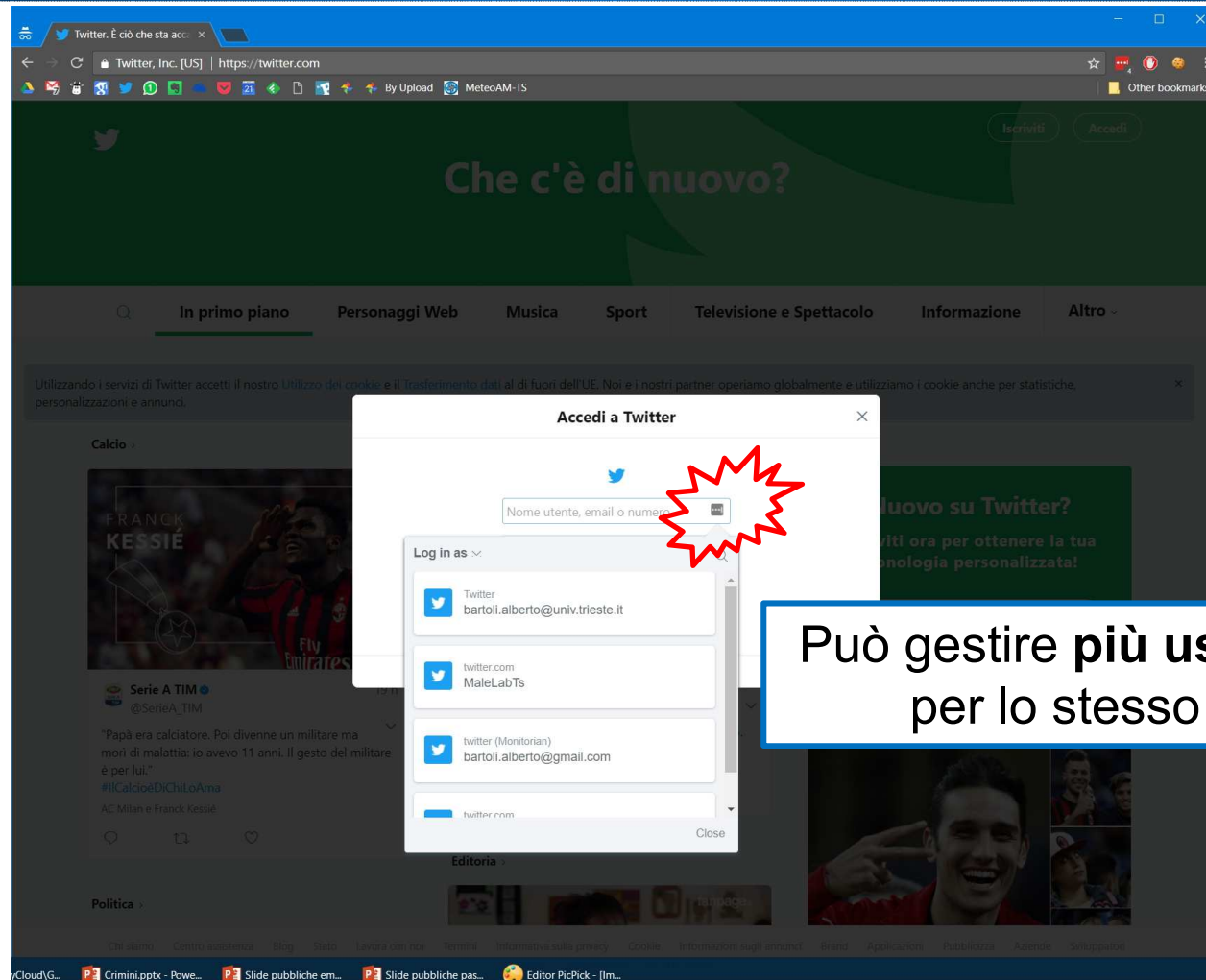
1. "Sufficientemente complicata"
 2. Diversa per ogni sito
- In teoria si
 - In pratica è quasi sempre **controproducente**
 - Spinge verso password semplici
 - Spinge verso password identica su ogni sito

Cammino verso la santità

1. Non inserirla in pagine a cui si arriva da link ricevuti
2. "Sufficientemente complicata"
3. Diversa su ogni sito

- Usare un programma **password manager**
- Genera e ricorda **tutte** le password
- Bloccato da **una** password
 - Risolve i problemi 2 e 3
 - Risolve (quasi del tutto) il problema 1
 - Devo ricordarne solo una

Esempio



Può gestire più username per lo stesso sito

Funzionalità utilissime

- **Sincronizza** automaticamente tutti i dispositivi (smartphone compreso)
- **Più username** per lo stesso sito
- Bloccato / sbloccato di **default** (smartphone /PC)
- Sblocco **aggiuntivo** per siti specifici (banca, paypal, postepay)
- Può memorizzare anche **altre informazioni** (numero carta credito, codice chiavi di casa)
- Permette **cambio automatico** di password su molti siti

Obiezione comune 1

- *Meglio scriverle se un foglietto*
- Verissimo
- Solo se si riescono a mantenere davvero **complicate ed univoche**
 - ...anche quando sono obbligato a rinnovarle

Obiezione comune 2

- *Se conosce tutto è un rischio*
- Verissimo
- Purtroppo in informatica il rischio zero non esiste
- Rischio "approccio quotidiano" è **molto più alto**
(ma **non ce ne rendiamo conto**)
- Migliore tecnologia esistente
 - Migliore non significa Perfetta

Obiezione comune 3

- *E' un software quindi può avere vulnerabilità*
- Verissimo
- Ma:
 - Risolvono le vulnerabilità nel giro di **poche ore**
 - Software **molto semplice**
 - Realizzati da aziende che **vivono di quello**
- Credenziali nel browser
 - Molto meglio di nulla...ma password manager è meglio

Obiezione comune 4 e 5

- *Quando sincronizza escono le password*
- *Se perdo il dispositivo ho perso le password*

- Si sblocca con una password (tutto crittato)
- Se l'ho scelta in modo adeguato
Allora non possono esserci problemi

Non prendo nessuna percentuale...

- [Lastpass](#) (gratuito) [1password](#) (3\$/mese) o altri
- Richiedono uno sforzo di apprendimento
- Ma sono alla portata di tutti: non sono per i tecnici

- Dovremo convivere con le password per molti anni
- Meglio fare uno sforzo iniziale

Ricapitolando

- **Non inserire password in dispositivi pubblici**
- **Non usare la stessa password su più siti**
 - Rischio **molto alto**
(ma non ce ne rendiamo conto)
- Usare password adeguate
 - 10/12 caratteri
 - Non riconducibili a noi o a “concetti tipici”
- Sforzarsi di usare un password manager