Parte 2:

Suggerimenti pratici

Email
Password

PC = Smartphone = Tablet = ...

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

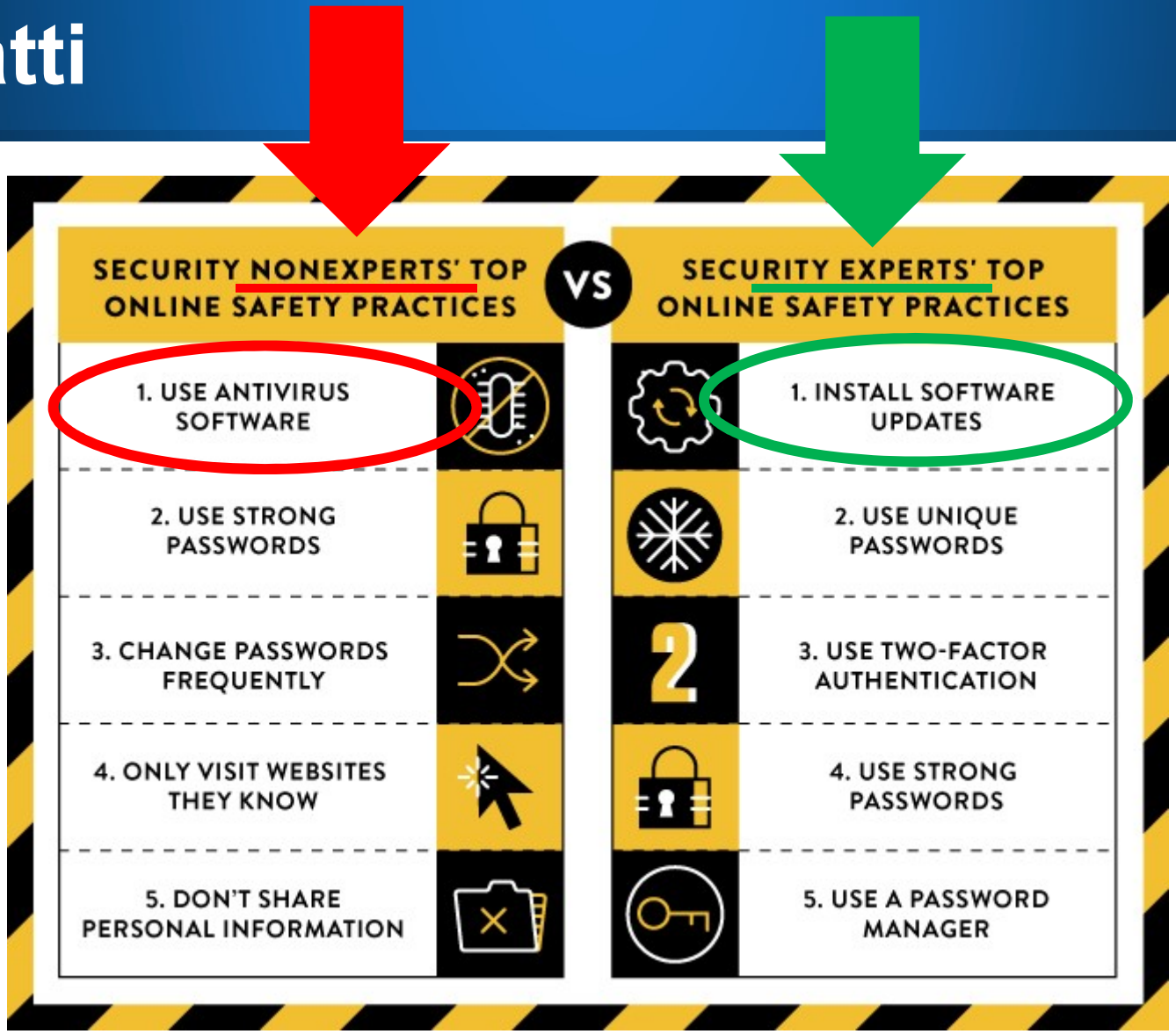
Difesa IMPORTANTISSIMA

- Aggiornamenti dei software (spesso) risolvono le vulnerabilità

- Mantenere i software **aggiornati**
- **Mai** disabilitare aggiornamenti **automatici**

- Usare Windows 7 / 8.1 è un (grosso) rischio

Infatti


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

Suggerimenti pratici

- Parte 1: Difenderci dagli attacchi
  - Come gestire gli email ricevuti
- Parte 2: Gestione delle nostre password
- Poco "affascinanti"
- Facili da **sottovalutare**
- **Enormemente importanti in pratica**

Parte 1:
Difenderci dagli attacchi

- Focus su attacchi:
  - **Comuni**
  - **Azioni utente decisive** per il successo (**tutti** basati sull'**inganno**)
- Email ricevuti (forme di "phishing")
- *"vabbè, chi vuoi che ci caschi..."*

Facili da sottovalutare, Enormemente importanti in pratica

The Hague, November 2019

- **Europol** stakeholders consistently highlight phishing or related attacks as the single **most common** attack vector with **65% of all reported cases**

- **Email** continues to be the **most widely used** vector with the **most severe** potential consequences.

google "Europol spear phishing report"

Attacchi email (phishing): Impatto

- Installazione **malware**
  (spesso è il primo step)
- Consegna username / **password** ad Attacker

- Iniziamo da installazione malware

Inganno 1:
Eseguo software SENZA SAPERLO (I)

- Attacker convince Utente ad **aprire file**
  - In generale innocuo...
  - ...ma se il programma che apre il file ha vulnerabilità?

- Metodo **comunissimo**: **Email ricevuti**
  - **Allegato**
    (apro allegato ⇒ installo malware)

Inganno 1: Eseguo software SENZA SAPERLO (II)

- Attacker convince Utente a **visitare pagina web**
  - In generale innocuo...
  - ...ma se il browser ha vulnerabilità?

- Metodo **comunissimo**: **Email ricevuti**
  - **Link**
    (visito link ⇒ installo malware)

Ricordare sempre

- **UN click** può essere sufficiente per perdere il controllo del proprio dispositivo
  - ...senza notifiche

- **NON** si deve smettere di clickare
- Ma **prima** di clickare si deve **riflettere**

Perché la email è un metodo comunissimo?

- Tecnicamente semplicissimo:
  1. Ingannare sul **vero mittente**
  2. Replicare **aspetto email** di quel mittente
  3. Ingannare sul **vero contenuto** di allegati / link

Dato di fatto 1:
Ingannare sul vero Mittente

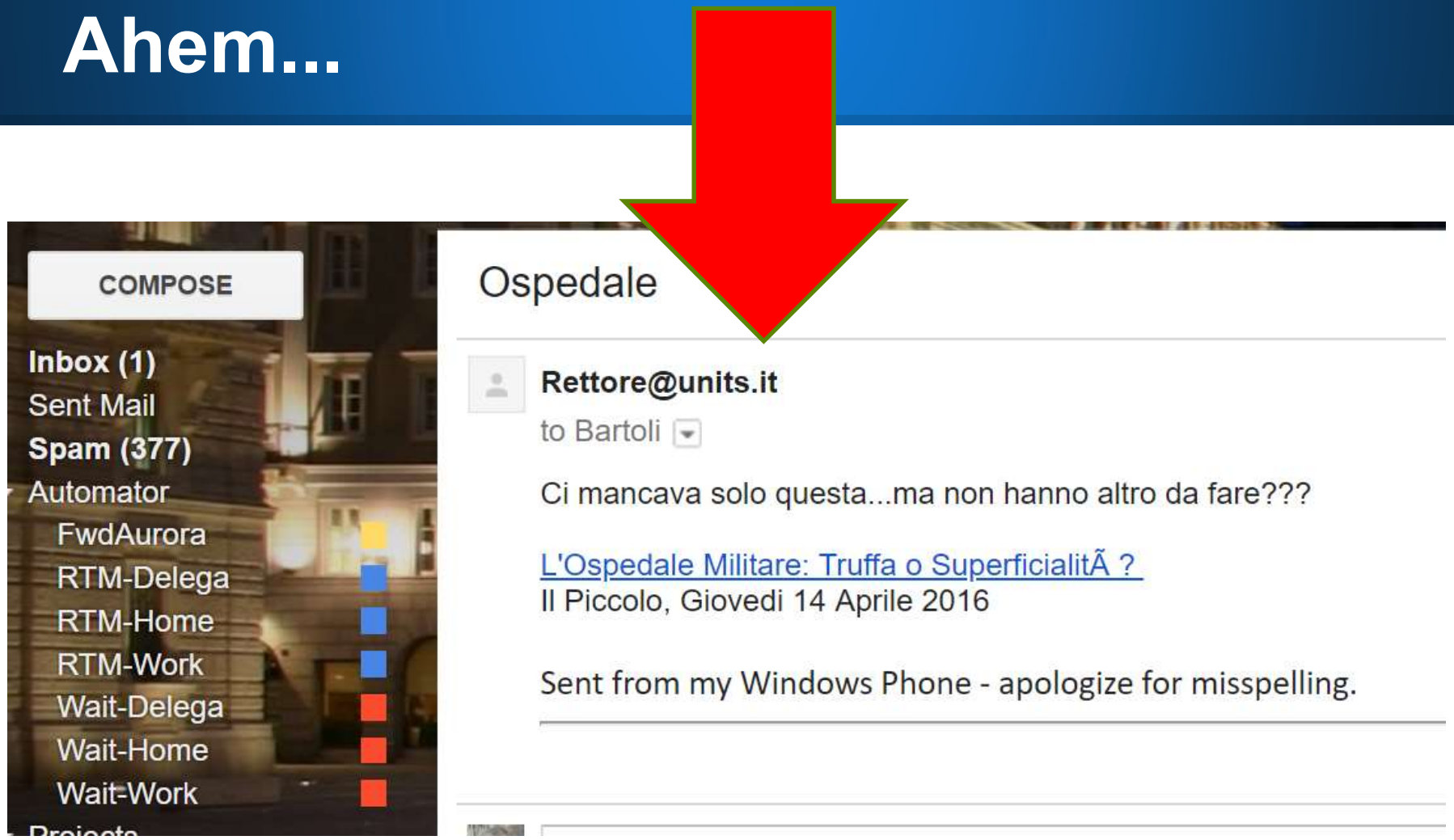
- **Chiunque** può inviarti con **poco sforzo** un email il cui mittente sembra:
  - Facebook
  - Netflix
  - Equitalia
  - Polizia di stato
  - Un tuo superiore / collega
  - Un amico
  - ...

Falso


From: Facebook [mailto:notification@faceboook.com]
Sent: 17 July 2012 15:38
To:
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 al Real Madrid...

Ahem...


COMPOSE
Inbox (1)
Sent Mail
Spam (377)
Automator
FwdAurora
RTM-Delega
RTM-Home
RTM-Work
Wait-Delega
Wait-Home
Wait-Work
Ospedale
Rettore@units.it
to Bartoli
Ci mancava solo questa...ma non hanno altro da fare???
L'Ospedale Militare: Truffa o SuperficialitÃ ?
Il Piccolo, Giovedi 14 Aprile 2016
Sent from my Windows Phone - apologize for misspelling.

Mittente: Falsificazione

Oggi falsificare un mittente `@units.it` non è più "molto semplice"

Mittente:
Inganni tecnicamente facilissimi

From: Roberto Di Lenarda <rettore@mail-units.it>

From: Roberto Di Lenarda <rettore@univ-trieste.it>

From: Roberto Di Lenarda <rettore@university-trieste.it>

From: DG <direttore.generale@univ-trieste.it>

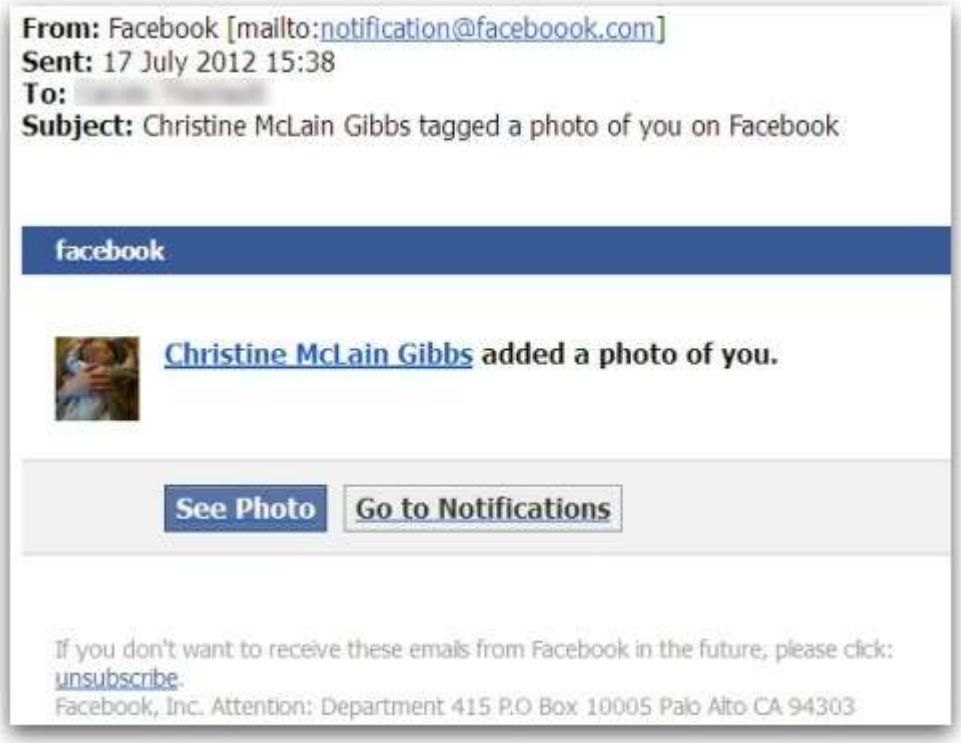
From: DG <direttore.generale@university-trieste.it>

From: Luciana Rozzini <dg@unitrieste.eu>

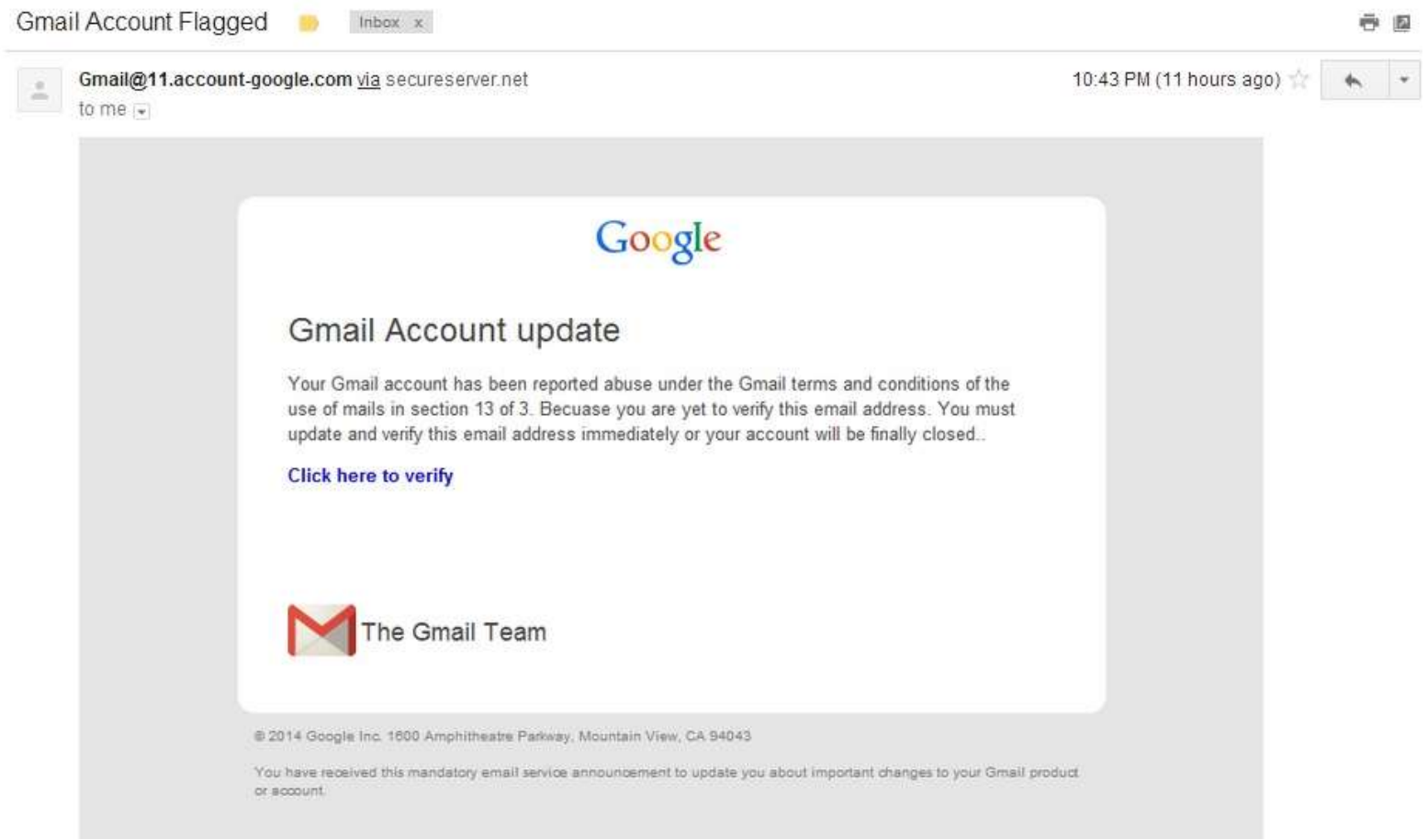
Dato di fatto 2: Replicare Aspetto

- Tecnicamente semplicissimo:
  1. Ingannare sul **vero mittente**
  2. Replicare **aspetto email** di quel mittente
  3. Ingannare sul **vero contenuto** di allegati / link

Falso... (Facebook)



Falso... (Google)



Falso... (Airbnb)

Da: Airbnb <admin@book-online.host>
Data: 22 febbraio 2018 00:44:11 CET
A: [redacted]
Oggetto: Message from Mairi about Peaceful cozy comfortable 6 bedroom house in Palma

airbnb

Message from Mairi

Mairi McMartin
Palma, Illes Balears, Spain
On Airbnb since 2018

Thank you for choosing my house for your trip in Palma.

Book your trip

Peaceful cozy comfortable 6 bedroom house in Palma ›
Entire villa

Check In
Wed, Jul 18, 2018

Check Out
Wed, Jul 25, 2018

Dato di fatto 3: Ingannare sul vero contenuto

- Tecnicamente semplicissimo:
  1. Ingannare sul **vero mittente**
  2. Replicare **aspetto email** di quel mittente
  3. Ingannare sul **vero contenuto** di allegati / link

Ingannare sul vero contenuto: ALLEGATI

- **Nome allegato** fa pensare ad un contenuto
- **Contenuto effettivo** può essere **diverso** (eventualmente malware)

```
verbale-21-Nov.pdf
risultato esami.docx
multa.pdf
...
```

Ingannare sul vero contenuto: LINK

- **Testo di un link** fa pensare ad un sito web
- **Sito web effettivo** può essere **diverso**
  1. Tentativo di iniezione malware nel browser
  2. ...

Hai visto? E' una vergogna!!!
Il Piccolo – Taglio agli stipendi in ateneo

Su quale sito vado se faccio click?

Solo 100 Biglietti gratis, affrettati su Ryanair!!!

Università di Trieste: i nuovi aumenti stipendiali

Attenzione alle email "sospette"!!!

- Quando ci sono una o più di queste condizioni:
  1. Email **inatteso**
  2. Contenuto **ci stimola moltissimo**
     (entusiasma / preoccupa / mette fretta)
  3. **Poco testo**

- **NON** clickare impulsivamente su allegati/link
- Prima di clickare **riflettere**

- Vediamo tra un momento come...

Esempio (I)

Da: Ufficio Polizia Giudiziaria Anticrimine <settore.tecnico.poliziag@gmail.com>

Inviato: mercoledì 27 aprile 2022 04:09

A: anticrimine.quest.convocazione@poliziadistato.it <anticrimine.quest.convocazione@poliziadistato.it>

Oggetto: ☆Settore Crimine Informatico - CONVOCAZIONE - (Prot.llo N°.IT243095reg.pg)☆

Salve,

VEDERE L'ALLEGATO

Siete invitati a rispondere il più presto possibile

CONVOCAZIONE POLIZIA GIUDIZIARIA

Cap. Giuseppe CAPUTO

Esempio (II)

POSTA CERTIFICATA: TRASMISSIONE ATTO DI STATO CIVILE PER TRASCRIZIONE

posta-c...@pec.actalis.it
to statocivile, me

Messaggio di posta certificata

Il giorno 18/11/2019 alle ore 09:43:06 (+0100) il messaggio
"TRASMISSIONE ATTO DI STATO CIVILE PER TRASCRIZIONE" è stato inviato da "anagrafe.corbara@asmepec.it"
indirizzato a:
statocivile@comune.modena.it bartoli.alberto@gmail.com
Il messaggio originale è incluso in allegato.
Identificativo messaggio: opec292.20191118094306.40828.522.1.62@pec.actalis.it
anagrafe.corbara@asmepec.it statocivile@comune.modena.it bartoli.alberto@gmail.com anagrafe.corbara@asmepec.it TRASMISSIONE

---------- Forwarded message ----------
From: "anagrafe.corbara" <anagrafe.corbara@asmepec.it>
To: statocivile@comune.modena.it
Cc: bartoli.alberto@gmail.com
Bcc:
Date: Mon, 18 Nov 2019 09:43:05 +0100
Subject: TRASMISSIONE ATTO DI STATO CIVILE PER TRASCRIZIONE

TRASMISSIONE ATTO DI STATO CIVILE PER TRASCRIZIONE

Regola 1

- Se arriva da un **sito** in cui abbiamo un **account**
- Allora andare sul sito **direttamente**
  - **Senza seguire link nell'email**
  - **Senza aprire allegato nell'email**

- La notifica/documento ci sarà di sicuro
- Se non c'è allora è un falso

- Non c'è il rischio di perdere notifiche importanti

Regola 2

- Se contiene una **notizia** molto interessante
- Allora cercarla ed andarci **direttamente**
  - **Senza seguire link nell'email**
  - **Senza aprire allegato nell'email**

- La notifica/documento ci sarà di sicuro
- Se non c'è allora è un falso

- Non c'è il rischio di perdere notifiche importanti

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
  - Non sono inattesi
  - Il rischio è sul **primo** email

- Più mi sorprende e stimola, più devo stare attento

Osservazione utile 2

- Mittente noto, affidabile

- **Non** deve essere utilizzato per decidere
  - Può essere semplice da **falsificare**
  - Potrei non averlo analizzato **correttamente** (`poliziaitaliana.it`? `pubblica-sicurezza.it`?)

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

Se qualcosa non mi quadra...

- Non è di un sito dove ho un account
- Non è una notizia che trovo su Internet
- Non è in una conversazione

1. Cercare di contattare il mittente **per altra via**
2. `sicurezzainformatica@units.it`
   - Risposta (tipicamente) in pochi minuti

- **NON** cliccare impulsivamente!

Whatspp / SMS:
Stessi problemi delle Email

Inganno 2:
Eseguo SW che sembra utile

- Attacker convince Utente ad eseguire software (**sembra utile** ma in realtà contiene malware)

- Metodi più comuni:
  - **Email ricevuto propone di eseguire software**
  - **Pagina web propone di eseguire software**

Mai INSTALLARE o ESEGUIRE sw su proposta web / email (I)

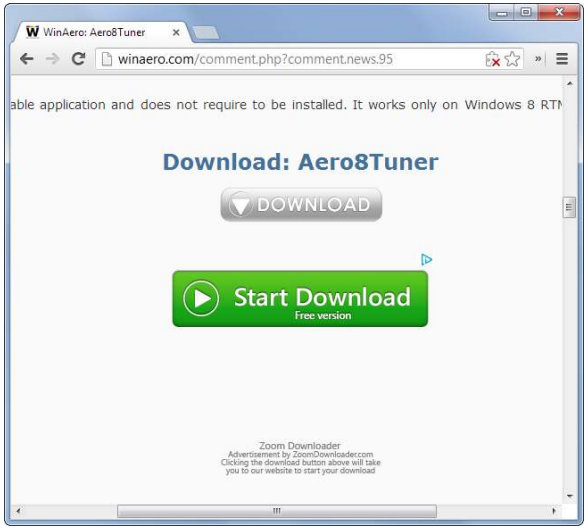
Security scan (?)

Mai INSTALLARE o ESEGUIRE sw su proposta web / email (II)

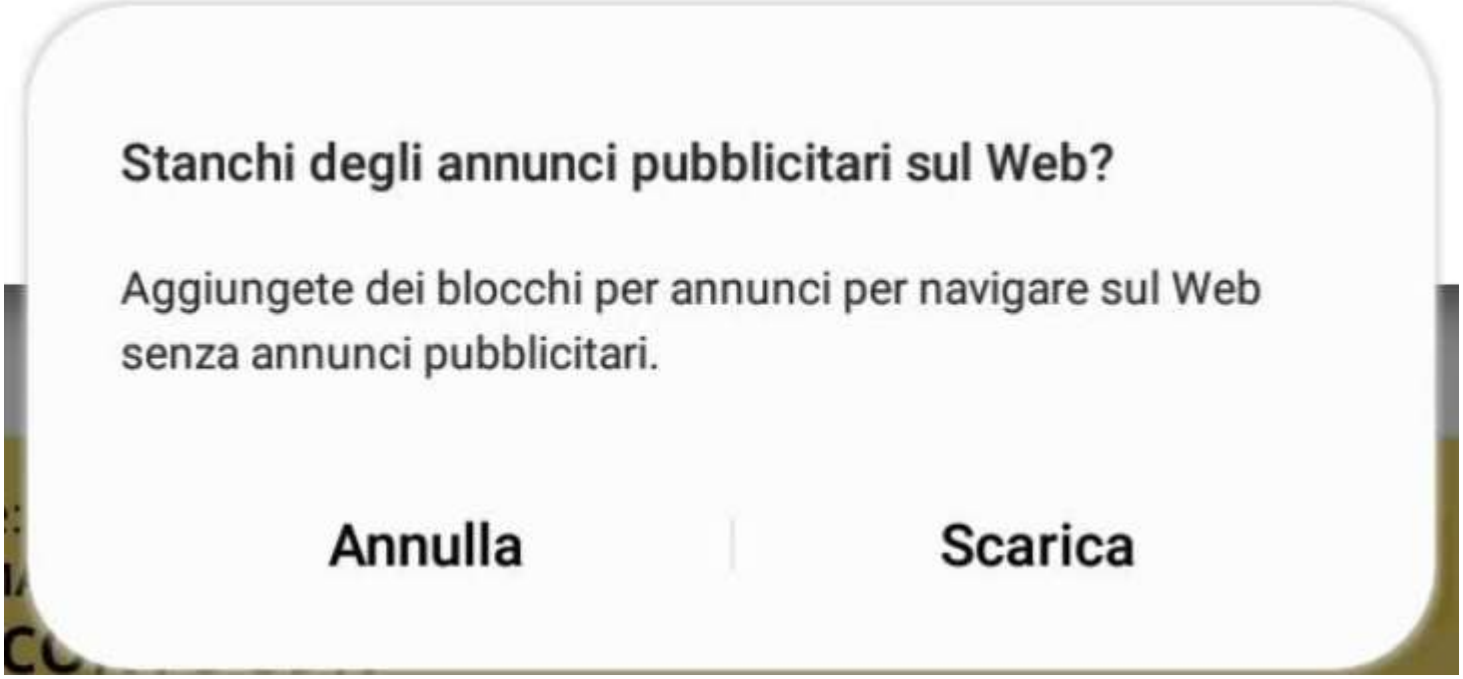
Video library missing (?)

Mai INSTALLARE o ESEGUIRE sw su proposta web / email (III)

Update necessario (?)



Mai INSTALLARE o ESEGUIRE sw su proposta web / email (IV)



Regola molto semplice (è sempre la stessa!)

- **Ogni** proposta di install / update **inattesa** deve essere **ignorata**
- **Chiudere** la pagina web / email ed infischiarsene della proposta

- Se proprio desidero aggiornare software:
  - Andare **direttamente** sul sito del produttore (Cercare su Google + Click sul risultato)
  - Maggiore garanzia di arrivare su pagina web legittima

Attacchi email (phishing): Impatto

- Installazione **malware** (spesso è il primo step)
- Consegna username / **password** ad Attacker

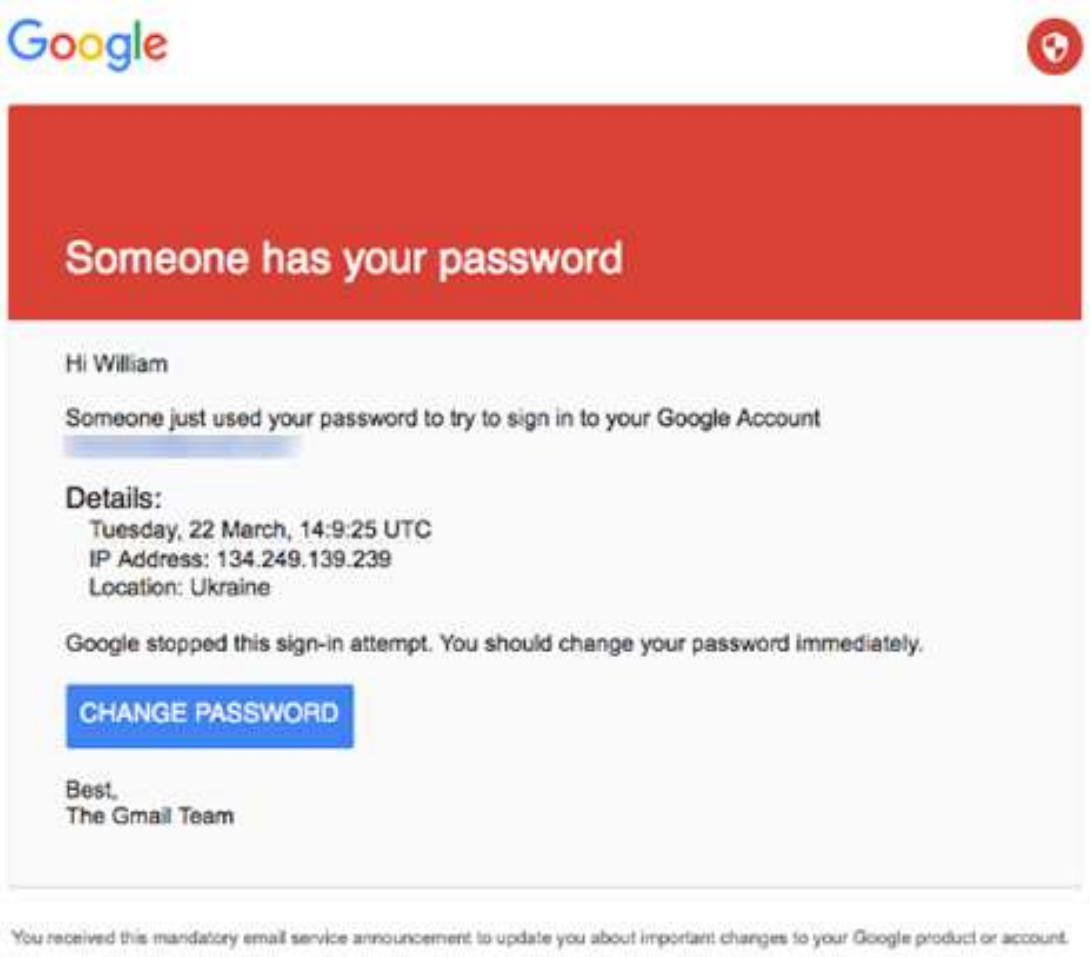
- Passiamo a consegna password ad Attacker...

Inganno 3

- Attacker convince Utente ad **inserire password** in pagina web **falsa**

- Metodo comunissimo:
  Email ricevuti

Come sono arrivati alle email di Hillary Clinton



Google

Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account

Details:
Tuesday, 22 March, 14:9:25 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

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

Dato di fatto 1

- **Testo di un link** fa pensare ad un sito web
- **Sito web effettivo** può essere diverso

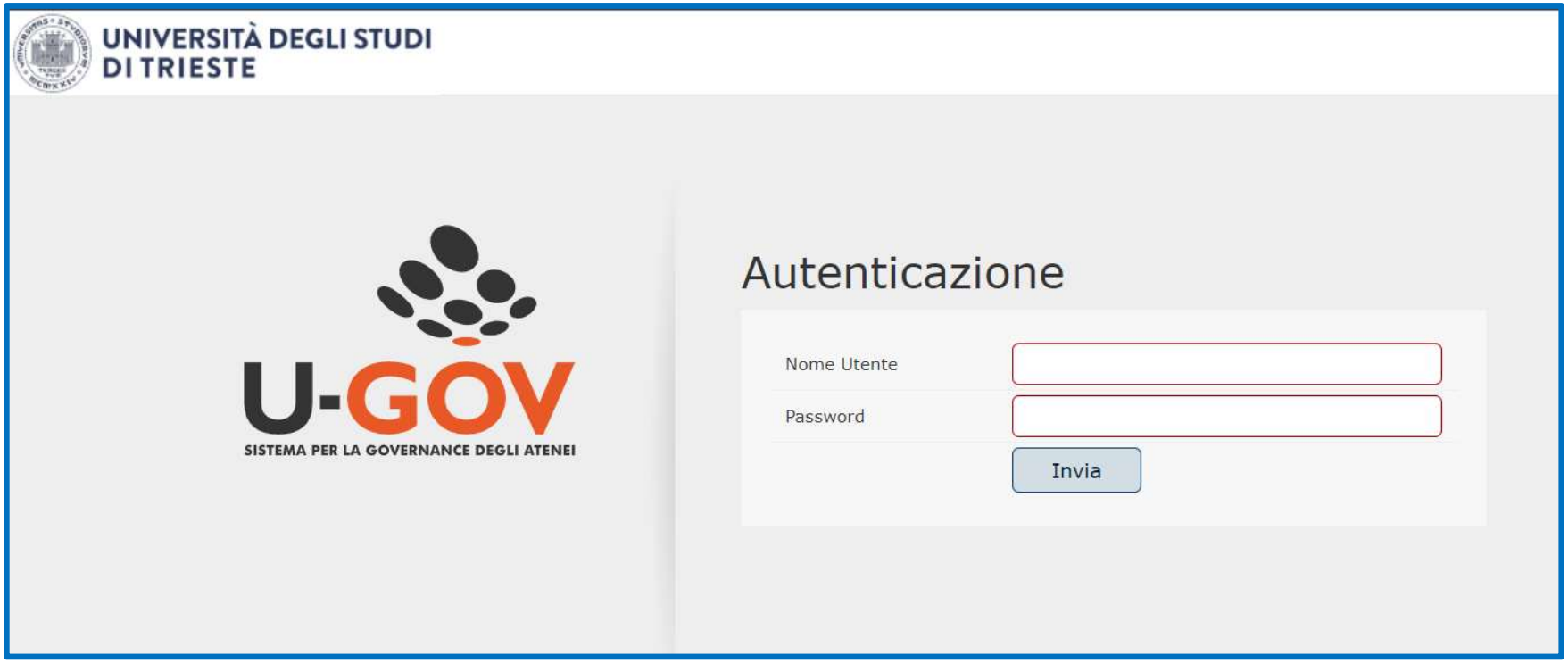
Timesheet U-GOV

Dato di fatto 2

- **Chiunque** può **replicare** con poco sforzo l'**aspetto** di un **sito web**

- …chiunque può creare una pagina web identica a:
  - Gestionale di lavoro
  - Unicredit
  - Facebook
  - Netflix
  - ...

Vera o falsa?


UNIVERSITÀ DEGLI STUDI
DI TRIESTE
U-GOV
SISTEMA PER LA GOVERNANCE DEGLI ATENEI
Autenticazione
Nome Utente
Password
Invia

Ricordare SEMPRE

- **L'aspetto** di una pagina web **non** è una prova della sua **autenticità**
- Dovrei verificare che il suo **indirizzo** (`http://`... o `https://`...) sia quello "giusto"
- Indirizzo sito web falso non è quello "giusto" (**diverso** da quello del sito web vero)

Grosso problema pratico

- Dovrei verificare che il suo **indirizzo** (http//... o /https...) sia quello "giusto"

1. **Molto più complicato** di quanto sembra
   - Potrei **non ricordarlo** o **non conoscerlo**
   - Rilevare un falso può essere **complicato**
   - Sugli **smartphone** è difficile vedere gli indirizzi
2. Ricordarsi di **verificare ogni volta** è **ancora più complicato**

Vero o falso? (I)

`https://promo.net/Ryanair`

`https://zara.offerteestate.com`

`https://ministero-interno.it`

`https://credit-agricole.it`

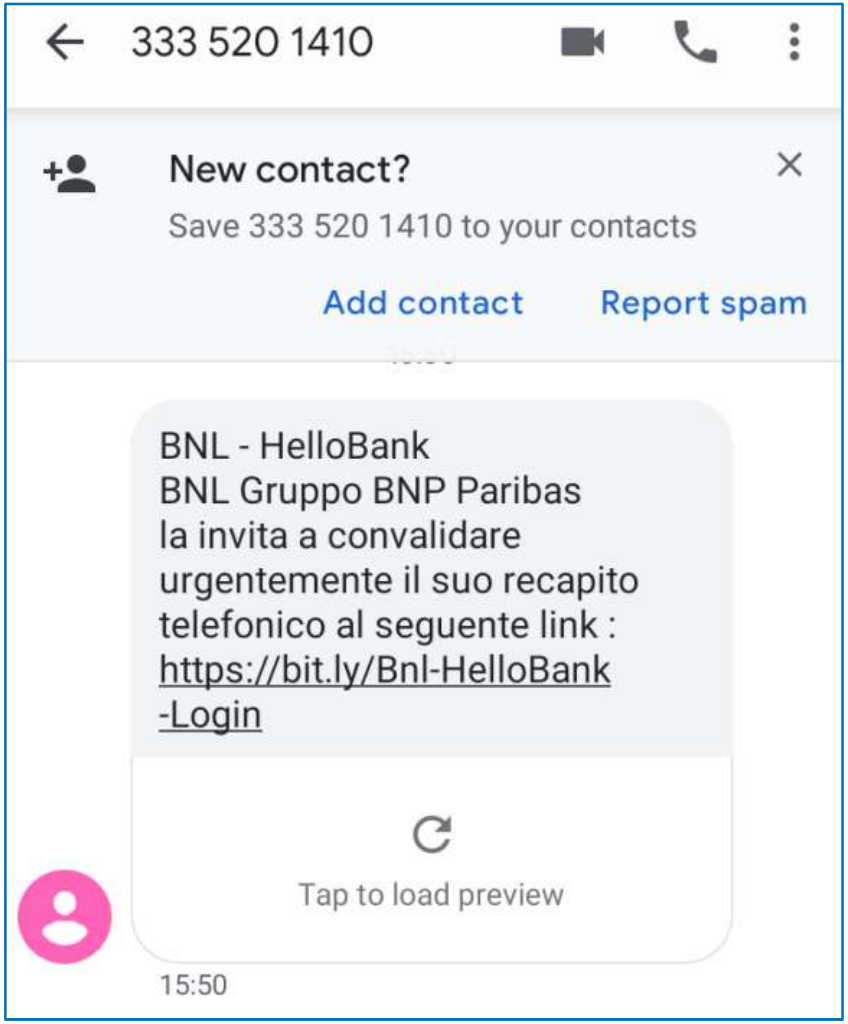
Vero o falso? (II)

```
https://units.u-web.cineca.it/appced
https://units-u.web-cineca.it/appced

https://www.units.u-gov.it/
https://www.units.ugov-cineca.it/

https://esse3-units.it/
https://units-cineca.it/cedolini
https://unitrieste.eu
```

Regola molto semplice

- **Mai** inserire credenziali in pagine web a cui si è arrivati con click su email (**MAI**)
- Arrivare a pagina di login sempre per altra via (**SEMPRE**)
  - Ricerca su Google (o analogo)
  - Browser del PC ha autocompletamento
  - Bookmark

Whatsapp / SMS: Stessi problemi



Spear Phishing (I)

- Phishing: **Stesso** email inviato a **molti** destinatari
- **Spear** Phishing: Email "**fatto appositamente**" per **uno / pochissimi** destinatari
  - Basta raccogliere qualche informazione (sito web organizzazione, LinkedIn, ...)

- Molto più complesso da rilevare
- Minaccia **reale**
  (vedi report Europol 2019)

Spear Phishing (II)

- **Spear** Phishing: Email "**fatto appositamente**" per uno/pochissimi destinatari

- Più costoso per Attacker
  $\Rightarrow$ Diretto verso i bersagli **più importanti**

- Chi occupa posizioni di rilievo (tecnico / organizzativo)
- ...e soprattutto **chi è vicino a loro**

- Deve essere **ancora più vigile!**

Attacchi: Ricapitolando

- Basati su **inganno**
  - **Email** metodo **efficacissimo**

- Mai clickare impulsivamente su link / allegati
  - Messaggi inattesi e stimolanti: sospetti! (specialmente gli **allegati**)
  - **Link**: sempre direttamente

- Mai "fidarsi" di pagine a cui si arriva via email
  - Arrivare a quelle pagine sempre direttamente
  - SMS / Whatsapp: idem

RIPETO:
Se qualcosa non mi quadra...

- Non è di un sito dove ho un account
- Non è una notizia che trovo su Internet
- Non è in una conversazione

1. Cercare di contattare il mittente **per altra via**
2. `sicurezzainformatica@units.it`
   - Risposta (tipicamente) in pochi minuti

- **NON** cliccare impulsivamente!

Suggerimenti pratici

- Parte 1: Difenderci dagli attacchi
  - Come gestire gli email ricevuti

- Parte 2: Gestione delle nostre password

- Poco "affascinanti"
- Facili da **sottovalutare**
- **Enormemente importanti in pratica**

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)
- **Moltissimi** attacchi reali si basano su furti di password

Cosa vedremo

1. Suggerimenti per (cercare di) **prevenire** il furto delle proprie password

2. Difesa in caso di **furti futuri**

- Cominciamo da 2

Autenticazione a due fattori / MFA / Verifica in due fasi

- Molti siti web offrono di associare il proprio **numero di telefono** al proprio account

- Autenticazione "conosci" + "possiedi":
  1. Utente inserisce Username+**Password**
  2. Utente inserisce OTP ricevuto via **SMS**

- Si può abilitare nel proprio account (**se disponibile**)
- Dettagli tecnici dipendono dal sito web

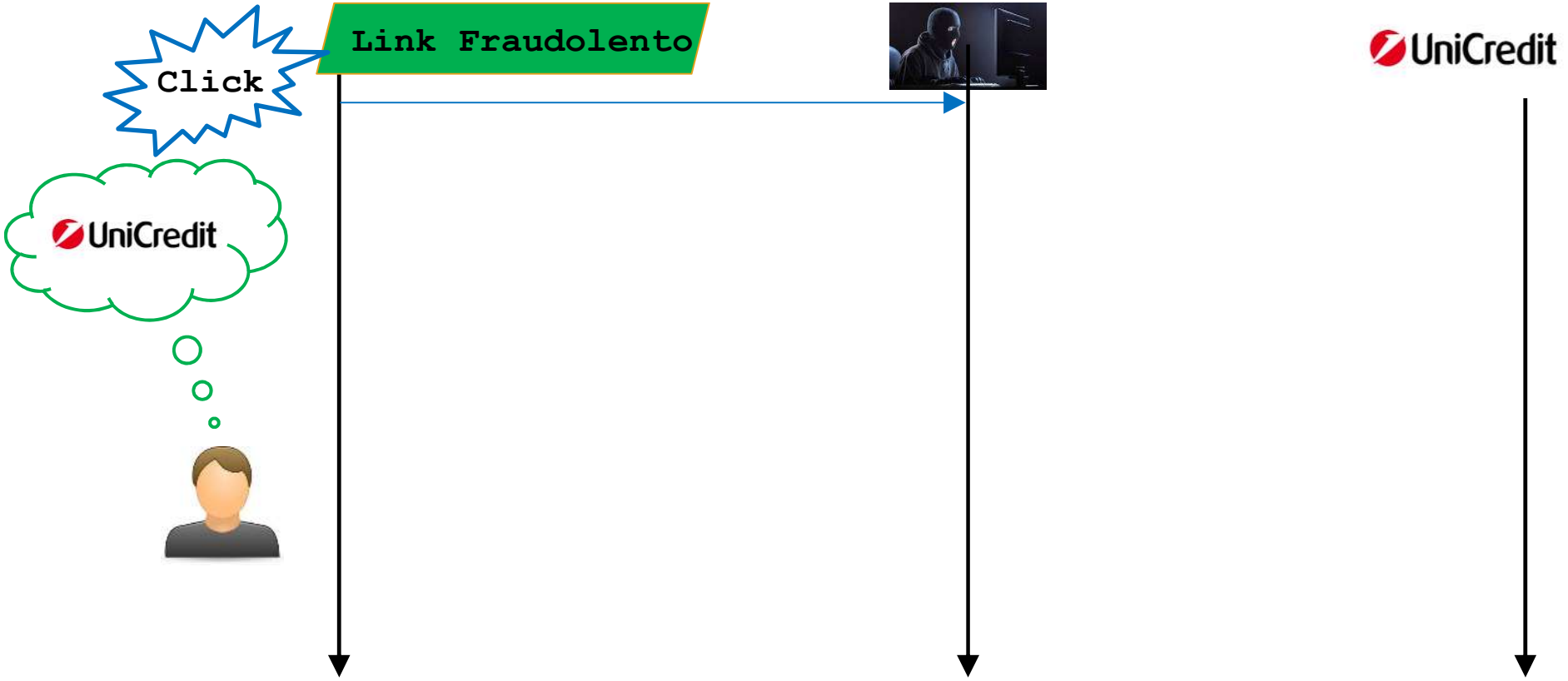
Difesa ENORMEMENTE efficace dai furti di password

- Autenticazione "conosci" + "possiedi":
  1. Utente inserisce Username+**Password**
  2. Utente inserisce OTP ricevuto via **SMS**

- Attacker con password **non** riesce ad entrare

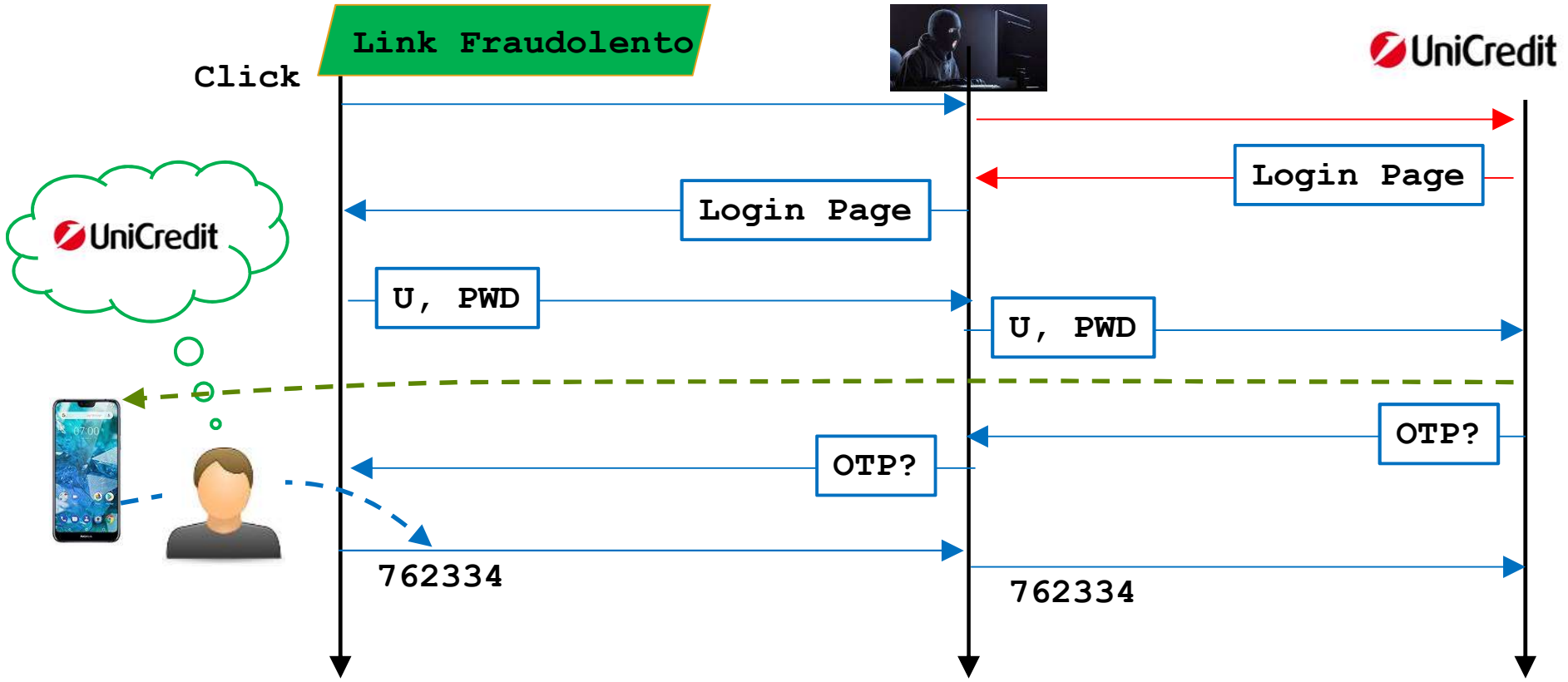
- **ABILITATELO!!! ABILITATELO!!! ABILITATELO!!!** (dove disponibile)

Difende dal phishing?



Pagina identica a quella vera
Indirizzo non vero

NON difende dal phishing!



Pagina identica a quella vera
Indirizzo non vero

"voice"- phishing!

"voice"- phishing!

Cybertruffa vocale: 20 mila euro spariti

Chiamata e invio di un codice sul cellulare che la vittima è invitata a leggere a voce alta ma è l'ok a una transazione

04 Agosto 2020 alle 15:38 | 2 minuti di lettura

IL PICCOLO

Una truffa della quale recentemente sono rimasti vittima anche dei **clienti triestini** di un istituto di credito.

Ricordare sempre

- **Mai** inserire credenziali in pagine web a cui si è arrivati con click su email (**MAI**)
- Arrivare a pagina di login sempre per altra via (**SEMPRE**)
- Autenticazione a più fattori:
  - Difende dal furto di password (**importantissimo**)
  - NON difende dal phishing

Cosa vedremo

1. Suggerimenti per (cercare di) **prevenire** il furto delle proprie password

2. Difesa in caso di **furti futuri**

- Passiamo a 1

Password:
Come può essere trafugata (I)

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

Come comportarsi

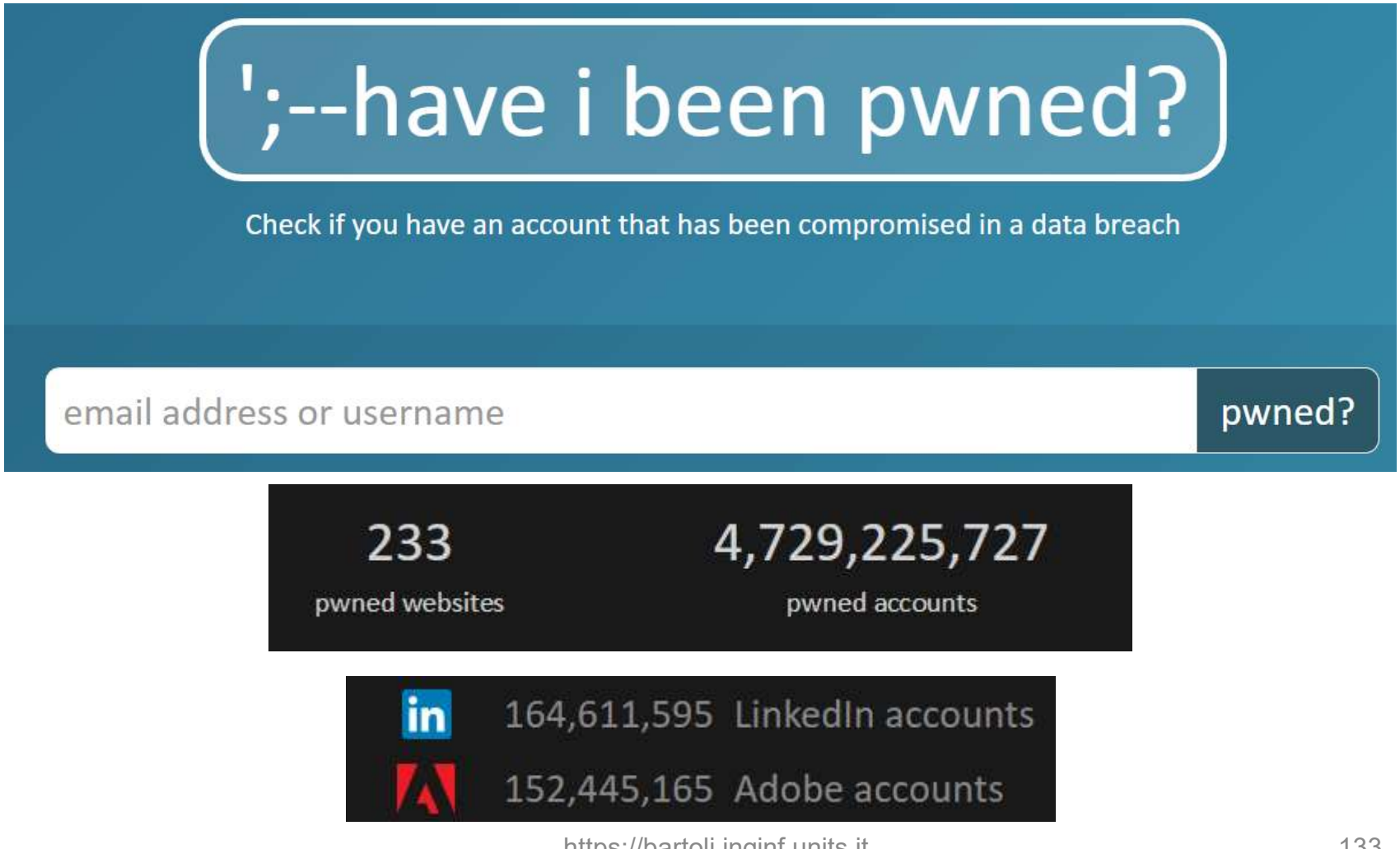
1. Malware sul dispositivo dove si inserisce
   - **Mai inserirla in dispositivi non nostri**
     - Caso comune: Postazioni pubbliche (hotel, aeroporti, ...)
     - Se proprio devo farlo, cambiarla il prima possibile (usando il **proprio** dispositivo)

2. Phishing
   - Già visto: mai fare login da link in email

Password:
Come può essere trafugata (II)

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

Furto sul server: Frequentissimo



La mia è stata rubata 9 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

Password:
Come dobbiamo SCEGLIERLE

1. Malware sul proprio dispositivo
2. Phishing

   Scelta ininfluente

3. Per tentativi

   "Sufficientemente **complicata**"

4. Furto sul server

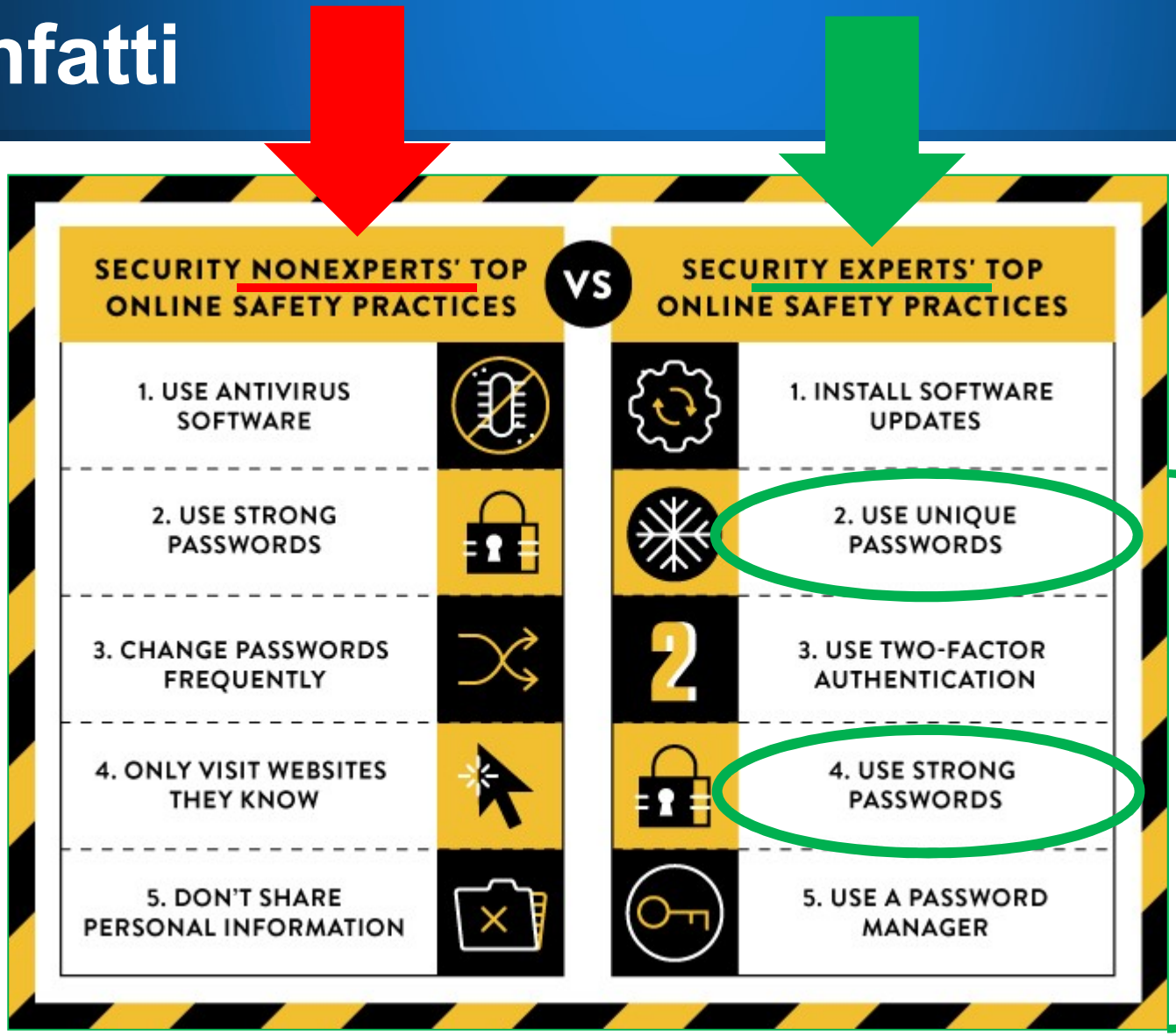
   Diversa per ogni sito

Nota bene

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

- **2 è MOLTO più importante di 1**

Infatti



password

Ma non dovrei cambiarle spesso?

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

- In teoria si
- In pratica è quasi sempre **controproducente**:
  Come le **ricordo**???
  - Spinge verso password **semplici**
  - Spinge verso password **identiche ovunque**

"Sufficientemente complicata": Che significa? (I)

1. Lunga almeno **10 caratteri** (12 è meglio)

2. Facile da **ricordare**
   - Niente caratteri speciali o cifre in posizioni strane
   - Se necessari, unico scopo è ricordarli (**non** renderla più complicata)

3. Non associabile a noi da **chi ci conosce**
   - Figli, compagni, date, scuole, indirizzi, cani/gatti...

"Sufficientemente complicata": Che significa? (II)

1. Lunga almeno 10/12 caratteri
2. Facile da ricordare
3. Non associabile a noi da chi ci conosce
4. 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": COME farlo

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

```
polentapistone
corallocontrattoago
suolaplatanocamino
```

- Meglio se di lingue diverse

```
suolaplatanolopta
```

"Diversa per ogni sito": COME farlo (ahia...!)

- **Ricordare** password diverse per **email** e **PC**
- Sono quelle di gran lunga più importanti

- Per tutte le altre:
  1. Ricordare con **metodo terra-terra**
     - Non ottimale ma molto meglio di quanto fatto di solito
     - Applicazione molto facile: niente scuse!
  2. Inserire nel **browser**
  3. Inserire in **password manager**
     - Il meglio ma è un pò più complicato

1) Ricordare con metodo terra-terra

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

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

- Molto meglio se **univoca** almeno nei gruppi 1 / 2

```
suolapistoneunits
suolapistonefacebook
corallocontrattopaypal
corallocontrattobanca
```

Obiezione comune

Che succede se dimentico password
*che ho **solo in testa**?*

1. Scrivetele in un foglietto
2. Custoditelo bene

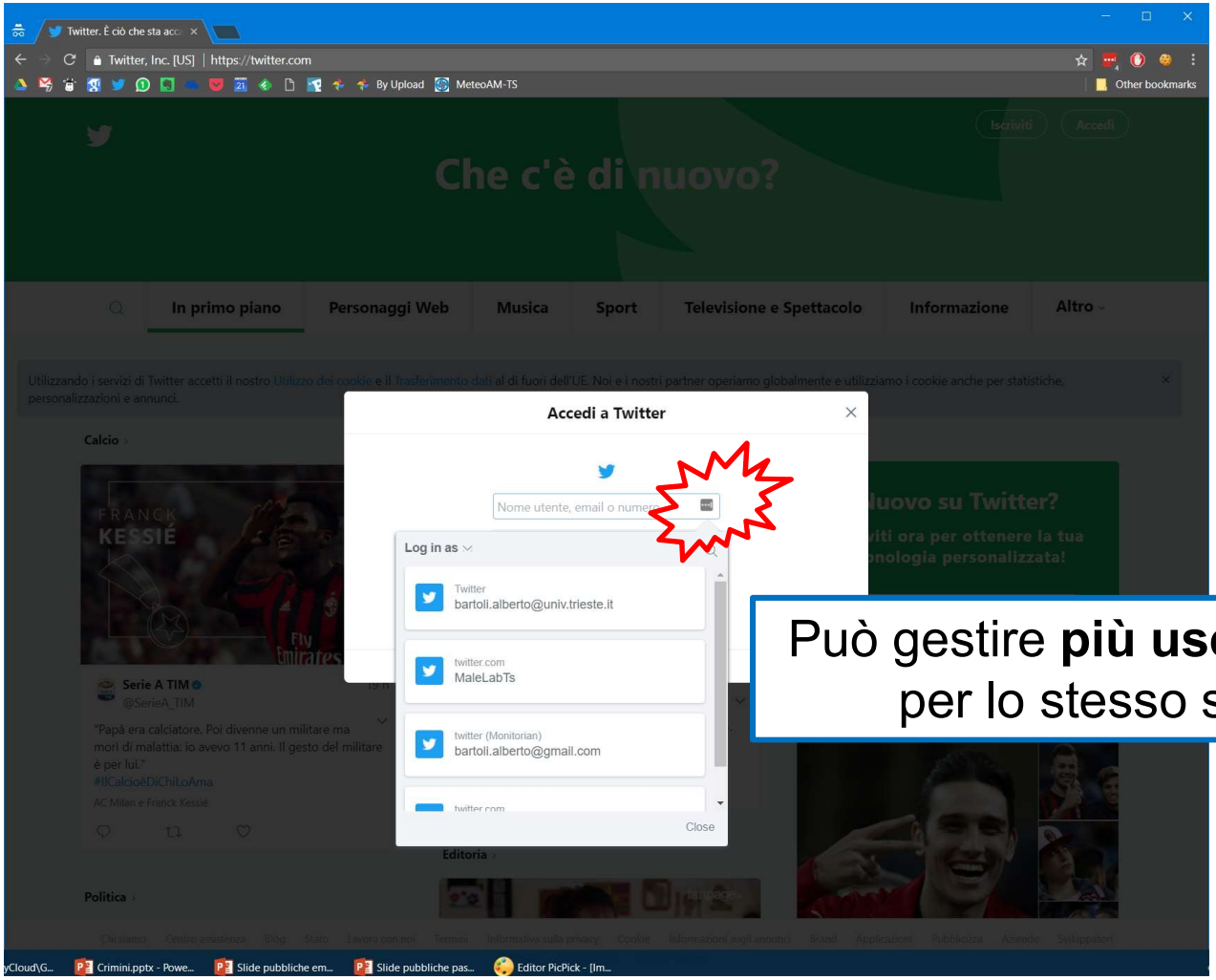
- Foglietto **solo** per emergenze
  (ed "eventi sfortunati"...)
- **NON** per consultazione sistematica !!!

2) Inserire in browser

- Ogni browser lo permette
  - Ricorda (ed eventualmente genera) **tutte** le password
  - Sincronizzazione automatica tra PC e smartphone

1. Arbitrariamente complesse
2. Univoche
3. Forte difesa dal phishing
   - Offre inserimento in pagina di login solo se indirizzo è quello "giusto"

Esempio:
Ha riconosciuto indirizzo vero



Può gestire **più username** per lo stesso sito

2) Inserire in browser: Rischio importante

- In pratica il browser è **sempre sbloccato**
- Accesso fisico al dispositivo?
  - Furto o smarrimento di portatile/smartphone?

Obiezione comune 1

Meglio scriverle su un foglietto per consultazione sistematica

- Verissimo
- **Solo** se si riescono a mantenere **complicate** ed **univoche**
- ...anche quando sono obbligato a **rinnovarle**
- ...ed abbiamo sempre il foglietto quando ci serve

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**)

Obiezione comune 3

E' un software quindi può avere vulnerabilità

- Verissimo
- Ma se hai un malware sulla tua macchina
  hai già perso
  (indipendentemente da come scegli le password)

3) Inserire in un Password Manager

- Estensione browser / smartphone app specializzata

- **Blocco** iniziale **configurabile** (smartphone / PC)
- Blocco **aggiuntivo** per siti specifici configurabile (banca, paypal, postepay)
- Può memorizzare **qualsiasi informazione** (numero bancomat, codice chiavi di casa)

2) Memorizzare nel browser: Rischio importante

- In pratica il browser è **sempre sbloccato**
- Accesso fisico al dispositivo?
  (es: furto o smarrimento di portatile/smartphone)
- Molto più semplice e pratico eliminare questo rischio
  - Browser sbloccato
  - Password manager bloccato

Su malware / vulnerabilità

E' un software quindi può avere vulnerabilità

- Verissimo
- Ma se hai un malware sulla tua macchina
  hai già perso
  (indipendentemente dale password)

- Malware specializzati molto meno comuni

- Software **molto semplice**
  (**molto** più semplice di un browser)
- Realizzati da aziende che **vivono di quello**
- Risolvono le vulnerabilità nel giro di **poche ore**

Non prendo nessuna percentuale...

- Bitwarden (gratuito)
- Lastpass, 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**
- **Abilitare autenticazione a due fattori**

- Usare password adeguate
  - Due-Tre sostantivi
  - Non riconducibili a noi o a “concetti tipici”

- Ricordarle per posta e PC
- Per tutte le altre: 3 metodi (password manager!)

Grazie per l'attenzione

`google "alberto bartoli trieste"`