Human Attacks – Social Engineering

Paolo PRINETTO
Director
CINI Cybersecurity National Laboratory
Paolo.Prinetto@polito.it
Mob. +39 335 227529

cini
Cybersecurity
National Lab
www.consorzio-cini.it

License & Disclaimer

License Information

This presentation is licensed under the Creative Commons BY-NC License

To view a copy of the license, visit:

http://creativecommons.org/licenses/by-nc/3.0/legalcode

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Acknowledgments

Thanks

- The presentation includes material from several contributors, whose valuable help is here acknowledged and highly appreciated.

Contributors

- CyberChallenge.IT
- Giuseppe AIRO' FARULLA
- Alessandro ARMANDO
- Roberto BALDONI
- Rocco DE NICOLA
- Arturo DI CORINTO
- Giorgio DI NATALE
- Eugene KASPERSKY
- Rosario PUGLIESE
- Francesco VESTITO
- Stefano ZANERO

© CINI - 2019

Ranking

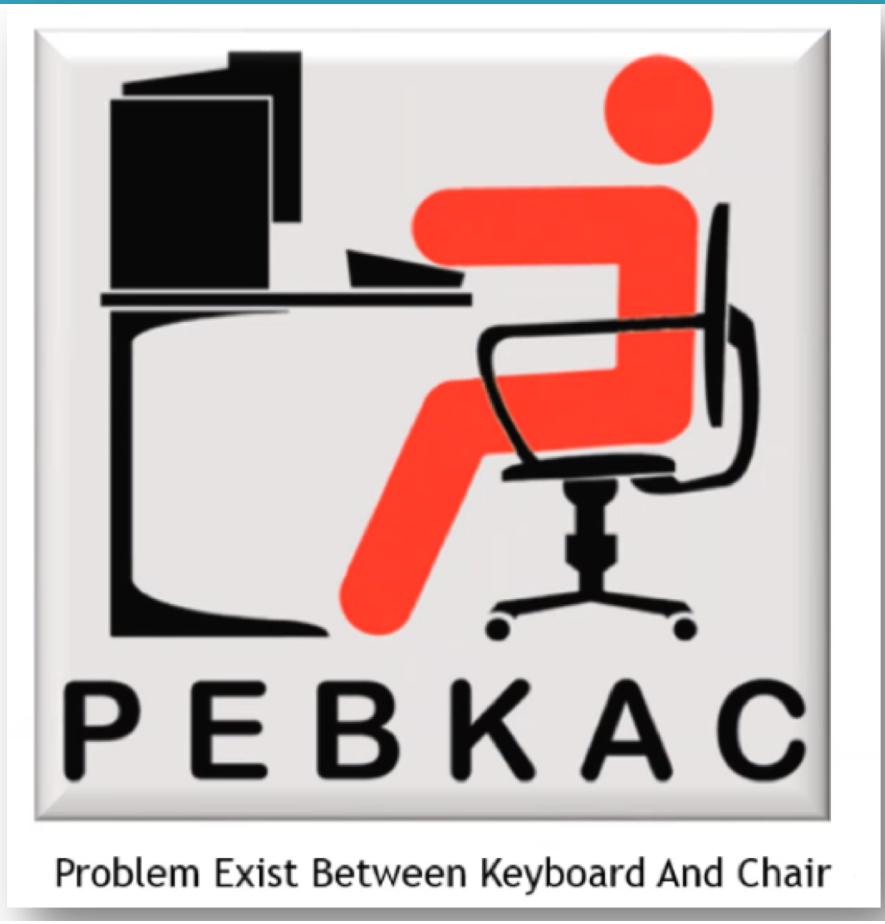
Fattore umano

Aspetti organizzativi

Aspetti tecnologici (HW/SW)

© CINI - 2019

L’uomo è sempre l’anello debole !!



© CINI - 2019

Weakest Link

- No matter how strong are your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software
  - …

Weakest Link

- No matter how strong are your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software
  - …
- You are the weakest link in computer security!

Weakest Link

- No matter how strong are your:
  - Firewalls
  - Intrusion Detection Systems
  - Cryptography
  - Anti-virus software
  - …
- You are the weakest link in computer security!
- People are more vulnerable than computers!

L'uomo è sempre l'anello debole !!

Fake News

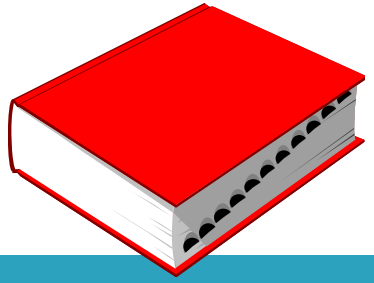
- L'uomo viene attaccato tramite la rete: si sfruttano la pervasività, la velocità della rete e … l'ignoranza degli utenti

Social Engineering

- Le strutture in rete vengono attaccate usando l'uomo per acquisire informazioni utili allo scopo

© CINI - 2019

Social engineering



- Tentativo di influenzare una persona con l'obiettivo finale di:
  - farle rivelare informazioni confidenziali
  - farla agire in maniera tale da consentire accesso o uso non autorizzato di sistemi, reti o informazioni
- Dalla attività criminale classica eredita il concetto di *inganno*.

© CINI - 2019

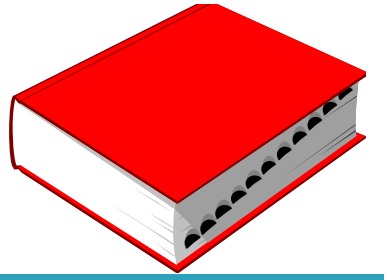
Social Engineering - Target

- Target primario è il personale di help desk, segretariale o di supporto

Social Engineering - Target

- Target primario è il personale di help desk, segretariale o di supporto
- Perché spendere tempo nel cercare le vulnerabilità di un sistema, quando con l'inganno se ne può ottenere la password?

Social Engineering



"Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology"

Kevin D. Mitnick & William L. Simon - Art of Deception

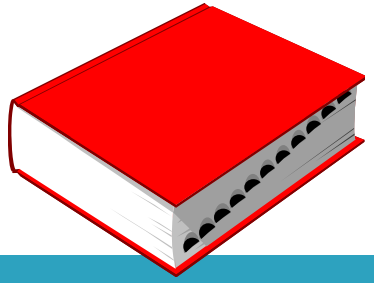
© CINI - 2019

Types of *Social Engineering*

- *Phishing*
  - Fraudulently obtaining private information
- *Physical Access*
  - Unauthorize building access
- *Stealing important informations or documents*
  - Dumpster diving
- *Baiting*
  - Real world trojan horse

© CINI - 2019

Phishing



- Truffa via Internet in cui l'aggressore cerca di ingannare la vittima inducendola a fornire informazioni personali, come ad esempio credenziali d'accesso, dettagli sul conto corrente bancario e sulle carte di credito.

Phishing – Come si realizza

- Tipicamente tramite l'invio, più o meno mirato, di e-mail che imitano nella grafica e nelle impostazioni siti bancari o postali con le quali si richiede di inviare dati personali

Unusual, non-IC sender

From: Helpdesk [paulsmith@stp-mineral.com]
To: Undisclosed Recipients
Subject: UPGRADE ACCOUNT

Your email missing

Hello Customer,

Impersonal greeting

As part of our upgrades to new Office system we require to verfy your mailbox.

Poor spelling and clunky grammar

Please click here to submit your updated information.

http://192.168.235.144/submit/index.jsp

Hover over the link to check the URL. Not an Imperial address.

If action is not taken by you we will terminate your online services.

Threats / urgency

Thank you
ITS Help Desk Administrator

Generic signature, no contact information

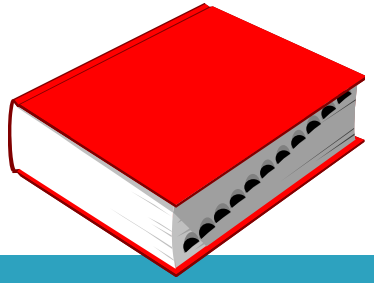
"Il tuo pc e' bloccato", La polizia postale segnala nuova ondata truffe

Navigando può capitare di trovarsi di fronte ad una schermata di (finto) blocco, accompagnata dall'invito a chiamare un numero di telefono per ottenere supporto tecnico online: è un raggiro

Lo leggo dopo | 27 aprile 2019

ABBONATI A Rep:

Whaling



- Attacchi di phishing diretti specificamente verso senior executive e altre persone di elevato profilo del mondo della finanza e dell'industria in generale.

Whaling

- Attacchi di phishing diretti specificamente verso senior executive e altre persone di elevato profilo del mondo della finanza e dell'industria in generale.
- Il termine whaling (da whale - balena) è stato coniato per questi tipi di attacco per evidenziare la "grandezza" e l'importanza degli obbiettivi

Phishing

«È interessante notare quanto è creativa la gente quando si tratta di inventare modi subdoli per ottenere quanto le pare …

Dovete usare la medesima creatività per proteggere i sistemi informatici nei settori pubblici e privati.

Perciò quando pensate alle politiche di sicurezza delle vostre aziende siate creativi e pensate fuori dal sentiero tracciato.»

Stealing important documents

How

- Dumpster diving
  - Looking through the "trash" for sensitive information
- Stealing important documents
  - Can take documents off someone's desk

Prevention

- Lock your files and dumpsters securely
- Easy secure document destruction (Erase magnetic media)

© CINI - 2019

Baiting

How

- Real world Trojan horse
- Uses physical media
- Relies on greed/curiosity of victim (e.g., attacker puts a legitimate or curious label to gain interest)

Example

- Attacker leaves a malware infected USB drive in a location sure to be found

Social Engineering Prevention

- Social engineering cannot be blocked by technology alone

Social Engineering Prevention

- You need:

Social Engineering Prevention

- You need:
  - Training and Education

Social Engineering Prevention

- You need:
  - Training and Education
- Cyber-Hygiene
- Courses
- Continuous Education
- Training
- Frameworks
- Certifications
- …

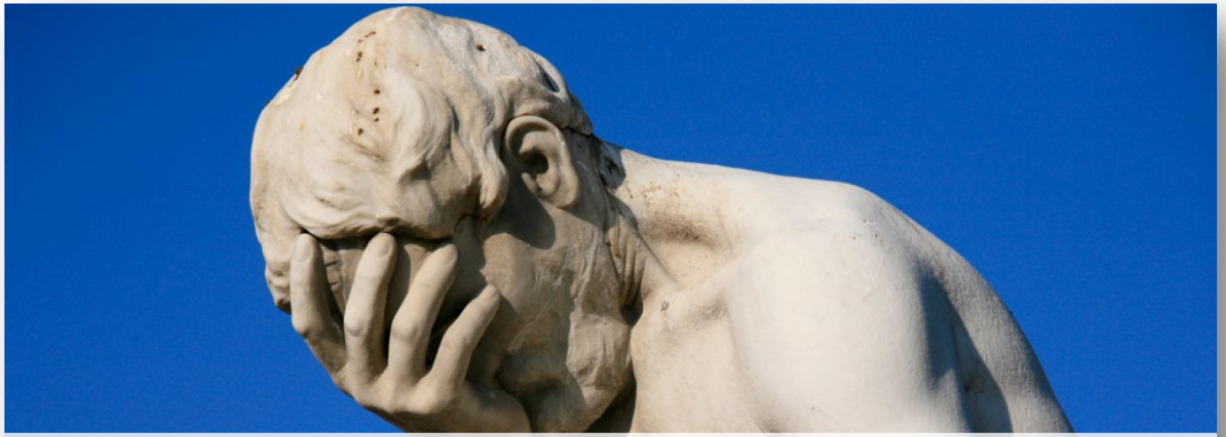
Social Engineering Prevention

- You need:
  - Training and Education

- Cyber-Hygiene
- Courses
- Continuous Education
- Training
- Frameworks
- Certifications
- …

1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321



17 INTERNET

Ecco la lista delle password più usate del 2016: accertatevi che non ci sia anche la vostra!

1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

Avete cambiato la password del router WiFi di casa o che usate in viaggio?

I changed all my passwords to "incorrect".
So whenever I forget, it will
tell me "Your password is incorrect."

© CINI - 2019

JIMMY
Kimmel
LIVE!
abc
WEEKNIGHTS 11:35|10:35c

Difese

Cultura e Spirito Critico

- Non esistono *pallottole d'argento*: serve dubitare, chiedersi a chi serve, cercare le fonti, …

Conoscenza Tecnologica

- Bisogna essere coscienti dei pericoli a cui si è esposti e ai quali si può esporre altri: servono
  - *cyber-hygiene*
  - *media literacy*

© CINI - 2019

Il ruolo della legge

La California 'banna' le password facili (admin, 12345) per contrastare gli hacker

> *Per contrastare il crimine informatico la California ha approvato una legge che renderà illegale per le aziende di elettronica utilizzare password predefinite semplici come "password" o "admin" a partire dal 2020.*

di Piero Boccellato | @pieroboccellato | 8 ottobre 2018, ore 11:30

Regole di buon senso

Accetta ai criminali informatici di aprire tutti i propri account online

L' **83%** delle persone non usa un indirizzo e-mail separato per gli acquisti online

Riufiuta un facile percorso al criminale informatico

Utilizzare indirizzi e-mail diversi per i diversi account

Accetta a un criminale informatico di ripulirci il conto in banca

Il **74%** delle persone utilizza una carta di debito per i pagamenti online

Riufiuta ai criminali informatici di accedere al proprio patrimonio

Utilizzare una carta di credito a parte con un limite di spesa contenuto

Accetta ai criminali informatici di cancellare tutti i file del proprio computer

Il **69%** delle persone non esegue con regolarità il backup dei dati

Riufiuta ai criminali informatici di distruggere dati non replicabili

Eseguire con regolarità i backup (e utilizzarli anche come prova)

Accetta a un criminale informatico di ipotizzare la propria password

Il **62%** delle persone non cambia password frequentemente, né usa password complesse

Riufiuta a un criminale informatico un facile accesso

Utilizzare password complesse per ciascun account online e aggiornarle di frequente

Accetta a un criminale informatico di attirare l'utente in un falso sito Web

Il **60%** delle persone non utilizza un indicatore di ricerca sicura con il browser

Riufiuta a un criminale informatico l'accesso ai propri clic

Esplorare Internet in tutta sicurezza con un adeguato software di protezione

© CINI - 2019

Social Engineering Prevention

- You need:
  - Training and Education
  - Awareness

Social Engineering Prevention

- You need:
  - Training and Education
  - Awareness
- Be suspicious of unsolicited phone calls, visits, or email from individuals asking about internal information
- Do not provide personal or company's information unless authority of person is verified

Social Engineering Prevention

- You need:
  - Training and Education
  - Awareness
  - Policies

© CINI - 2019

Social Engineering Prevention

- You need:
  - Training and Education
  - Awareness
  - Policies
- Do not allow to divulge private information
- Prevents employees from being socially pressured or tricked
- Need to know

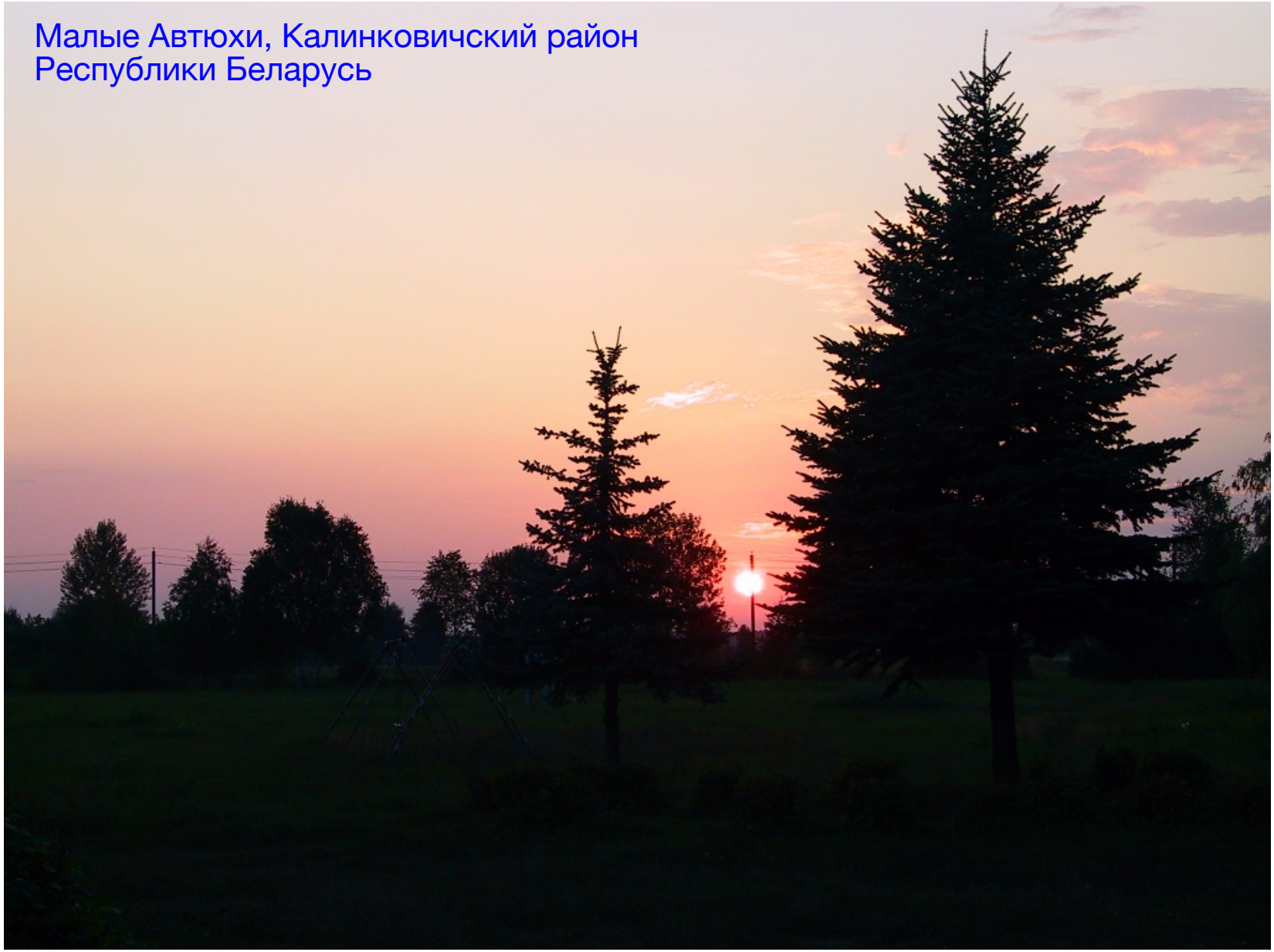
© CINI - 2019

Social Engineering Prevention

- You need:
  - Training and Education
  - Awareness
  - Policies
  - 3rd Party support

Social Engineering Prevention

- You need:
  - Training and Education
  - Awareness
  - Policies
  - 3rd Party support
- Have a third party come to your company and:
  - attempt to hack into your network
  - Detect problems people have with security
- Bug Bounty Programs & Ethical Hacker
- Attempt to glean information from employees using social engineering



Paolo PRINETTO

Director
CINI Cybersecurity National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

cini
Cybersecurity
National Lab

www.consorzio-cini.it