Le basi del social engineering

Giovanni Possemato 05-06-2020

www.presentationgo.com

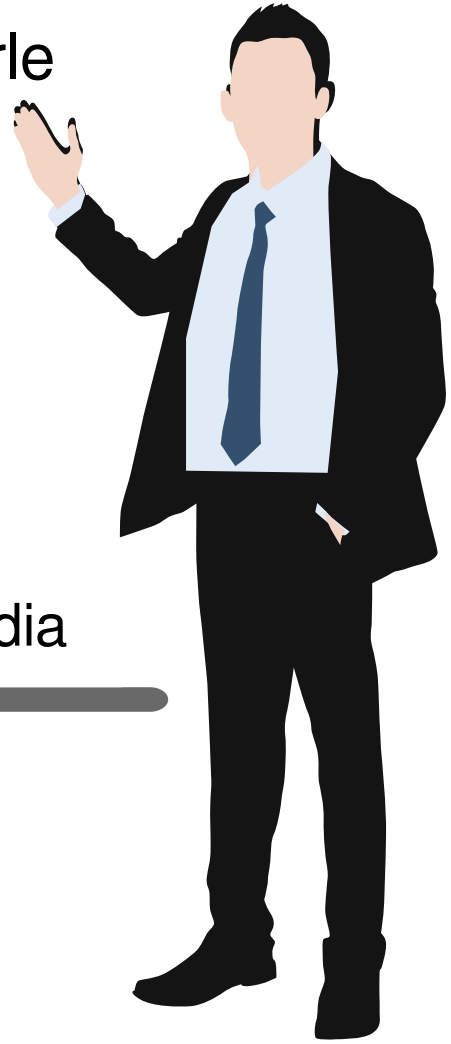
Cosa è il Social Engineering

È l’arte di manipolare le persone in modo tale da farle fare azioni che altrimenti non farebbero.

Kevin Mitnik

John Thomas Draper

Wikipedia



www.presentationgo.com

Cosa è il Social Engineering

Perché dovrebbero mirare a me?

- Per utilizzare l'infrastruttura per attacchi più grandi
- Per rubare informazioni sui Clienti (da attaccare a sua volta)
- Per recuperare informazioni sul bersaglio principale
- ...

www.presentationgo.com

Dove sta il problema?

Dove sta il problema?

www.presentationgo.com

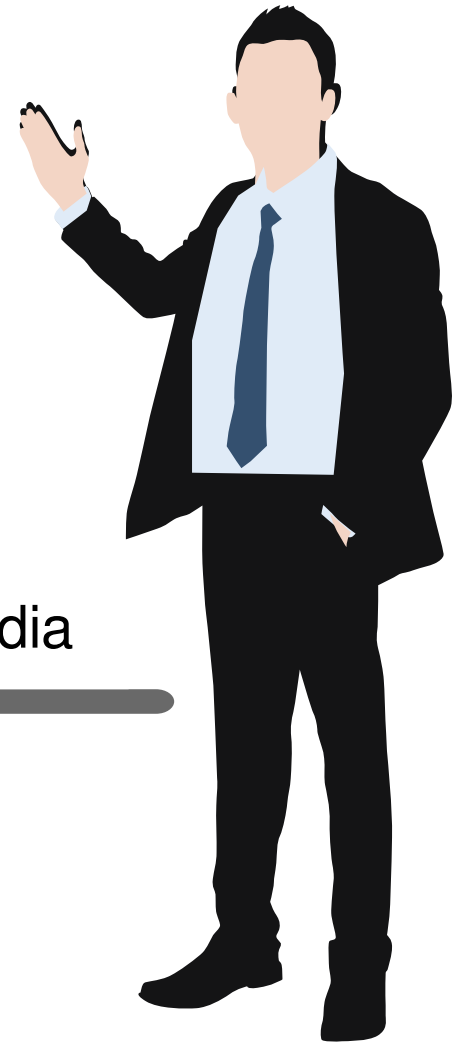
Dove sta il problema?

www.presentationgo.com

Cosa è il Social Engineering

Un white hat è un hacker in grado di introdursi nei sistemi al fine di aiutarne i proprietari a prendere coscienza di un problema di sicurezza

Wikipedia



www.presentationgo.com

Ethical Hacker

Facile fare un malware... il problema è come attivarlo!
Occorre convincere il malcapitato che il malware è un programma innocuo

Ma come?

www.presentationgo.com

Ethical Hacker

Un hacker etico dovrebbe:

- essere un buon programmatore per

1) creare/modificare/utilizzare malware
2) creare siti web finti
3) creare script, macro...
4) ...

www.presentationgo.com

Ethical Hacker

Un hacker etico dovrebbe:

- essere un bravo sistemista IT

1) conoscere il funzionamento degli O.S.
2) creare infrastrutture ad hoc (web, mail server...)
3) sapere come funzionano I protocolli (DNS,TCP..)

www.presentationgo.com

Ethical Hacker

Un hacker etico dovrebbe:

- avere tanta immaginazione

più immaginazione = più scenari possibili

www.presentationgo.com

Ethical Hacker

Un hacker etico dovrebbe

- Essere empatico...

www.presentationgo.com

Fasi di un attacco

Un penetration test di Social Engineering mira a sfruttare le vulnerabilità del fattore umano per eludere i sistemi di sicurezza e rubare informazioni o denaro dai sistemi della vittima.

www.presentationgo.com

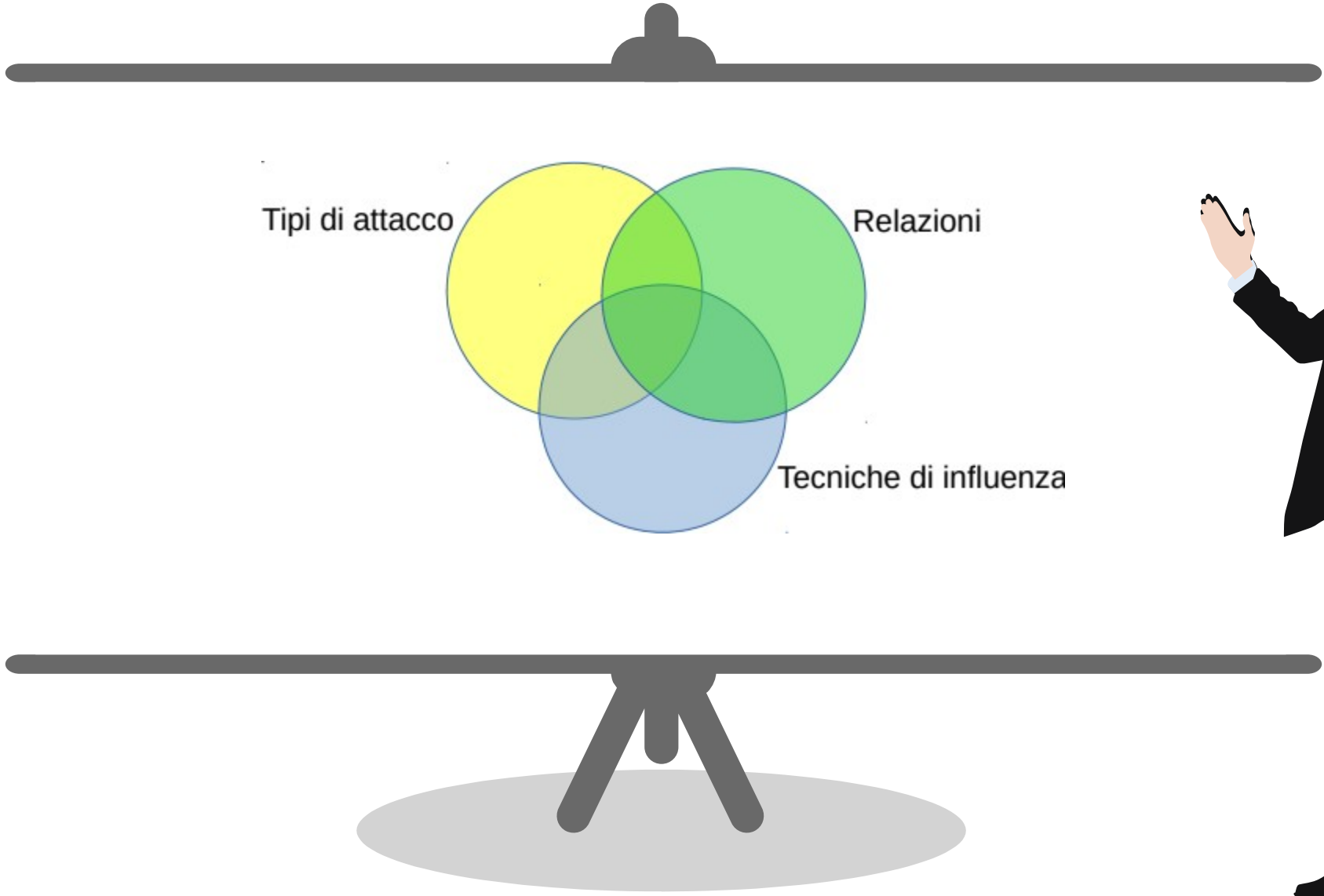
Fasi di un attacco

Pianificazione dell’attacco

- Raccolta delle informazioni
- Preparazione
- Sviluppo delle relazioni
- Sfruttamento delle relazioni
- Esfiltrazione delle informazioni
- Conclusioni finali

www.presentationgo.com

Fasi di un attacco



www.presentationgo.com

Raccolta delle informazioni

www.presentationgo.com

Raccolta delle informazioni

1) Osint (es. Maltego, the harvester...)

2) Social Network (da Linkedin si recupera buona parte dell'organigramma e delle relazioni)

3) Internet (il vostro sito da più informazioni di quello che pensate!)

www.presentationgo.com

Sviluppo delle relazioni

www.presentationgo.com

Sviluppo delle relazioni

Unidirezionali
L’hacker non stabilisce nessuna relazione con la vittima

1) l’hacker conosce l’identità della vittima
2) nessuna interazione con la vittima
3) finestra temporale di sfruttamento della relazione **molto lunga**

www.presentationgo.com

Sviluppo delle relazioni

Unidirezionali

Esempi:

- Spear Phishing
- Whaling
- Dumpster Divers
- Shoulder Surfing

www.presentationgo.com

Sviluppo delle relazioni

Bidirezionali

L’hacker tenta di instaurare una relazione
Con uno o più vittime.

- l’hacker conosce l’identità della vittima
- interazione intensa con la vittima
- finestra temporale di sfruttamento della relazione **medio**/**breve**

www.presentationgo.com

Sviluppo delle relazioni

Bidirezionali

Esempi

- Spear phishing
- Whaling
- Scam
- Vishing

www.presentationgo.com

Sviluppo delle relazioni

Indirette
L’hacker non stabilisce alcuna relazione con la vittima

- l’hacker non conosce l’identità della vittima
- nessuna interazione con la vittima
- finestra temporale di sfruttamento della relazione **molto breve**

www.presentationgo.com

Sviluppo delle relazioni

Indirette

Esempi

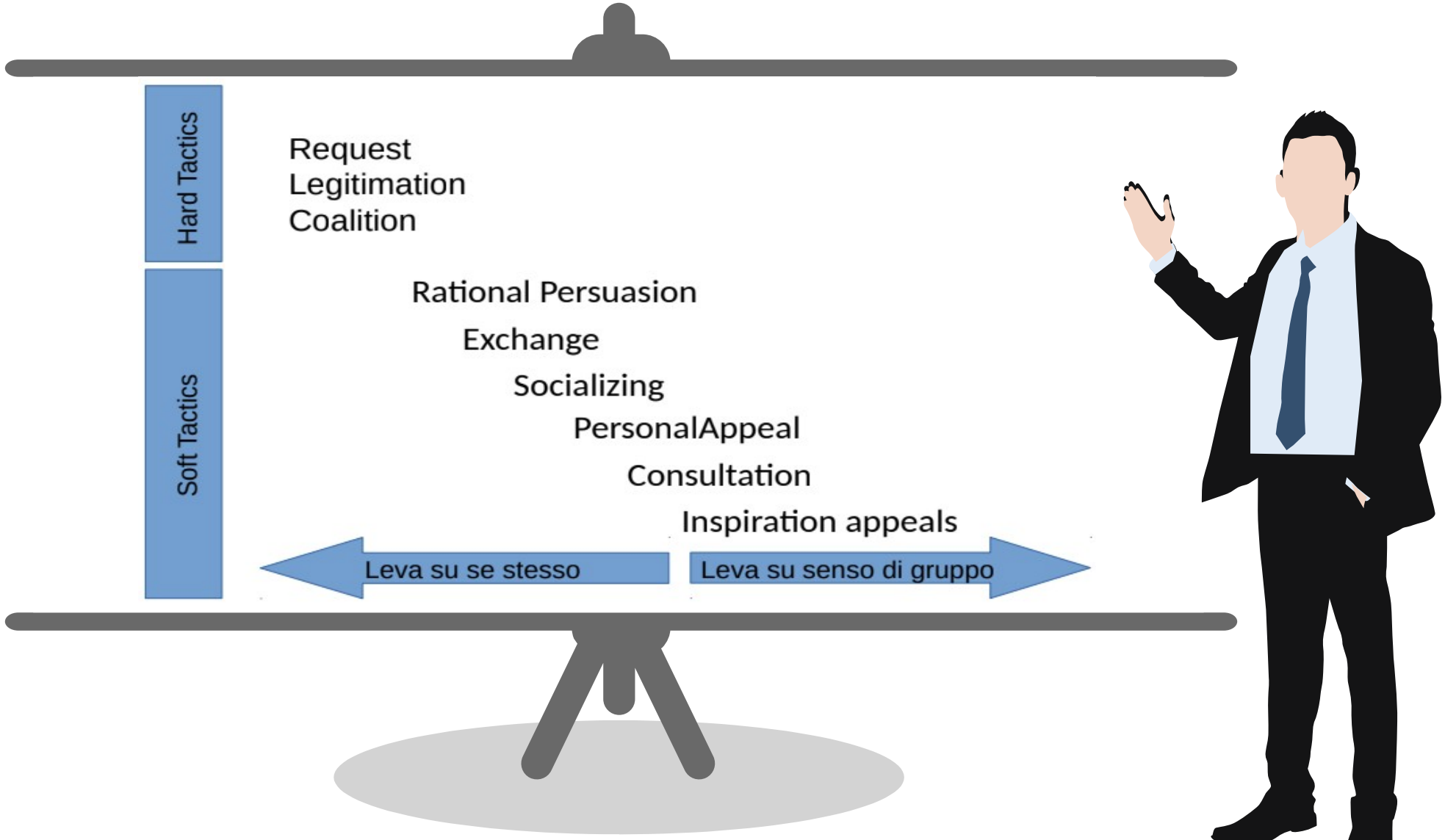
- SPAM
- Scam
- USB Drop Attack

www.presentationgo.com

Tecniche di influenza

www.presentationgo.com

Tecniche di influenza



www.presentationgo.com

Tecniche di influenza

Hard persuasion tactics (push)
Sono quelle tecniche che lasciano poco margine di libertà alla vittima

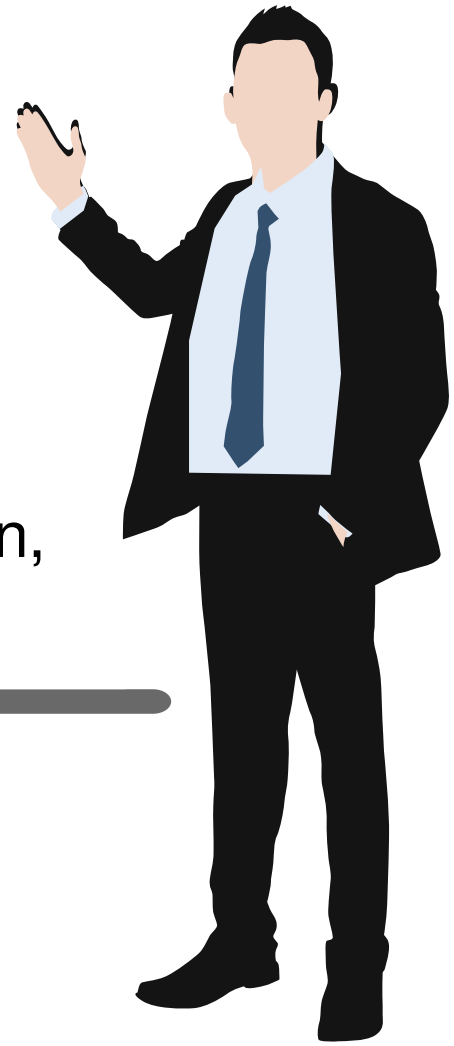
Soft persuasion tactics (pull)
Sono quelle tecniche che lasciano margine di libertà alla vittima

www.presentationgo.com

Tecniche di influenza

Positive persuasion tactics
Sono quelle tecniche che mantengono buono il rapporto con la vittima (es. rational persuasion, appeal, exchange collaboration)

Negative persuasion tactics
Sono quelle tecniche che insultano, rovinano la reputazione o insultano la vittima (es. legitimization, coalition, pressure)



www.presentationgo.com

Tecniche di influenza

Requesting

Si chiede direttamente un’azione alla vittima facendo leva sull’obbedienza o sulla convenienza ad esaudire la richiesta

www.presentationgo.com

Tecniche di influenza

Requesting

“Ciao, sono il nuovo responsabile del personale; per capire come vanno le cose in azienda, abbiamo creato un questionario per verificare la felicità del personale. Potresti compilare il sondaggio cliccando su questo link?”

www.presentationgo.com

Tecniche di influenza

Requesting

“Buongiorno, sono un impiegato del fisco ed abbiamo notato delle incongruenze nel suo ISEE di quest’anno. Ci occorrerebbero ulteriori informazioni per evadere la pratica. Le alleghiamo il questionario da compilare e rimandarci il prima possibile.”

www.presentationgo.com

Tecniche di influenza

Legitimating

“L’hacker fa leva su una posizione di potere per indurre la vittima a fare qualcosa”

www.presentationgo.com

Tecniche di influenza

Coalition

“Molto simile al legitimate, l’hacker chiede un’azione legittimando la richiesta con il fatto che è prassi comune che le altre persone lo fanno.
Social proof: la vittima è convinta che la richiesta è lecita in quanto “lo fanno tutti”

www.presentationgo.com

Tecniche di influenza

Coalition

“Ciao, di solito queste cose me le faceva Carlo, ma oggi non riesco a trovarlo.Potresti abilitarmi te l’account anche sul server XXX?, agli altri ci aveva già pensato Carlo”

www.presentationgo.com

Tecniche di influenza

Coalition

“Ciao, io e altre 100.000 persone abbiamo già aiutato l’associazione “Sgancia la grana”per aiutare gli orsi polari dall’estinzione. Fai come noi, aiuta donando a questo link...”

www.presentationgo.com

Tecniche di influenza

Rational Persuasion

Cerca di convincere la vittima che l’azione è legittima adducendo esempi convincenti

www.presentationgo.com

Tecniche di influenza

Rational Persuasion

“Aiutami a presentarmi alle prossime elezioni. Uno dei miei punti principali è evitare l’aumento delle tasse. Clicca qui per firmare la petizione”

www.presentationgo.com

Tecniche di influenza

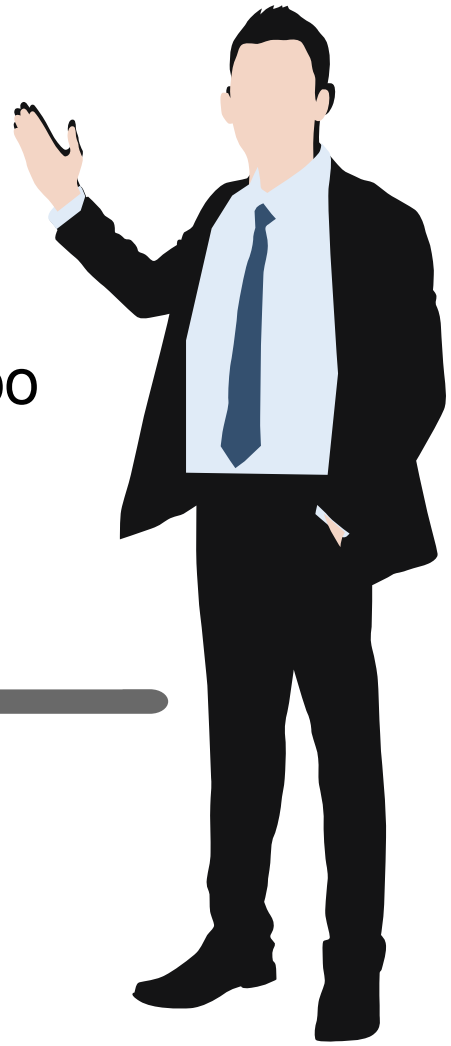
Exchanging
L’hacker aiuta la vittima risolvendo un problema (forse creato apposta) e poi chiede un’azione in cambio.
Quid pro quo:
la vittima è più disponibile a esaudire la richiesta, se riceve qualosa in cambio.

www.presentationgo.com

Tecniche di influenza

Exchanging

“Salve, sono del supporto del vostro sistema di posta elettronica, abbiamo appena rilevato un attacco al server. Siamo riusciti a bloccarlo senza farlo sapere troppo in giro, ma dovremmo accedere un momento al server per verificare. Puoi darci le credenziali?”

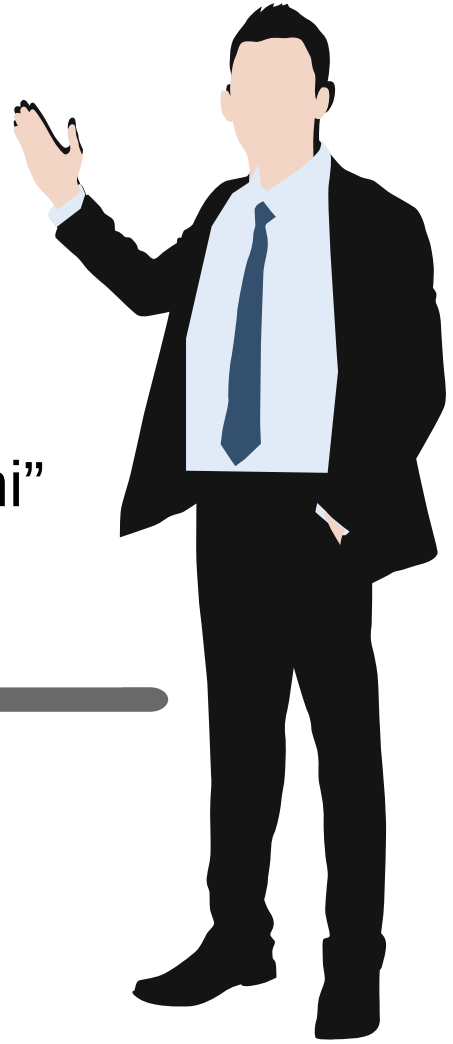


www.presentationgo.com

Tecniche di influenza

Quid pro quo

“Clicca QUI per vincere un sacco di premi”



www.presentationgo.com

Tecniche di influenza

Socializing
Costruire un’interazione amichevole con la vittima per convincerla ad eseguire la richiesta
Liking:
la vittima è più disponibile ad eseguire un’azione se la richiesta viene da una persona affascinante.

www.presentationgo.com

Tecniche di influenza

Socializing

“Clicca qui per vedere le mie foto...”
“Ciao, chattiamo...”

www.presentationgo.com

Tecniche di influenza

Personal Appeals
L’hacket chiede di eseguire un’azione come favore personale

Liking/Exchanging:
la vittima è più disponibile ad eseguire l’azione se questo serve ad ingraziarsi l’amico/a (liking) o il proprio capo (exchanging)

www.presentationgo.com

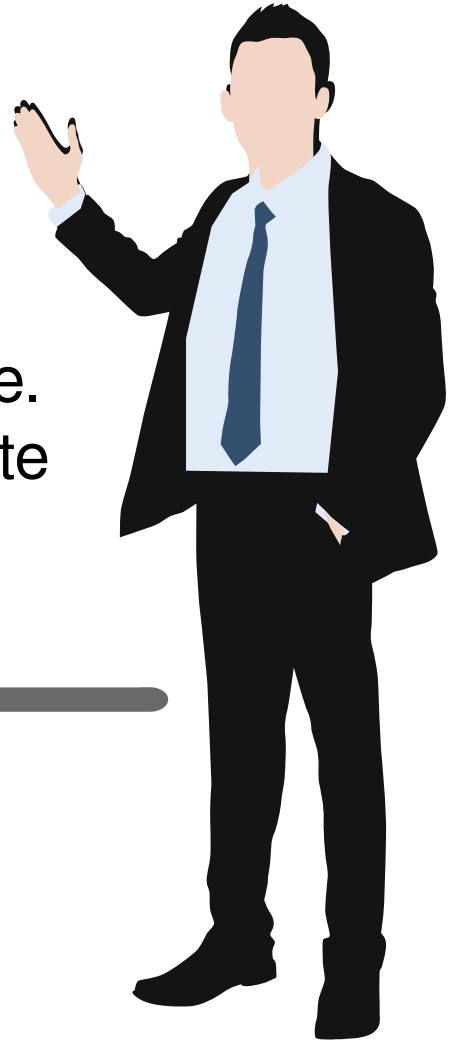
Tecniche di influenza

Personal Appeals
“Ciao, puoi aiutarmi a compilare QUESTO documento? Devo farlo entro domani e da solo non ce la faccio. Lo apprezzerei molto!”

www.presentationgo.com

Tecniche di influenza

Personal Appeals
“Puoi mandarmi dei soldi per arrivare in Italia? Te li ridarò appena arriverò lì da te. Te ne sarò eternamente grata”



Tecniche di influenza

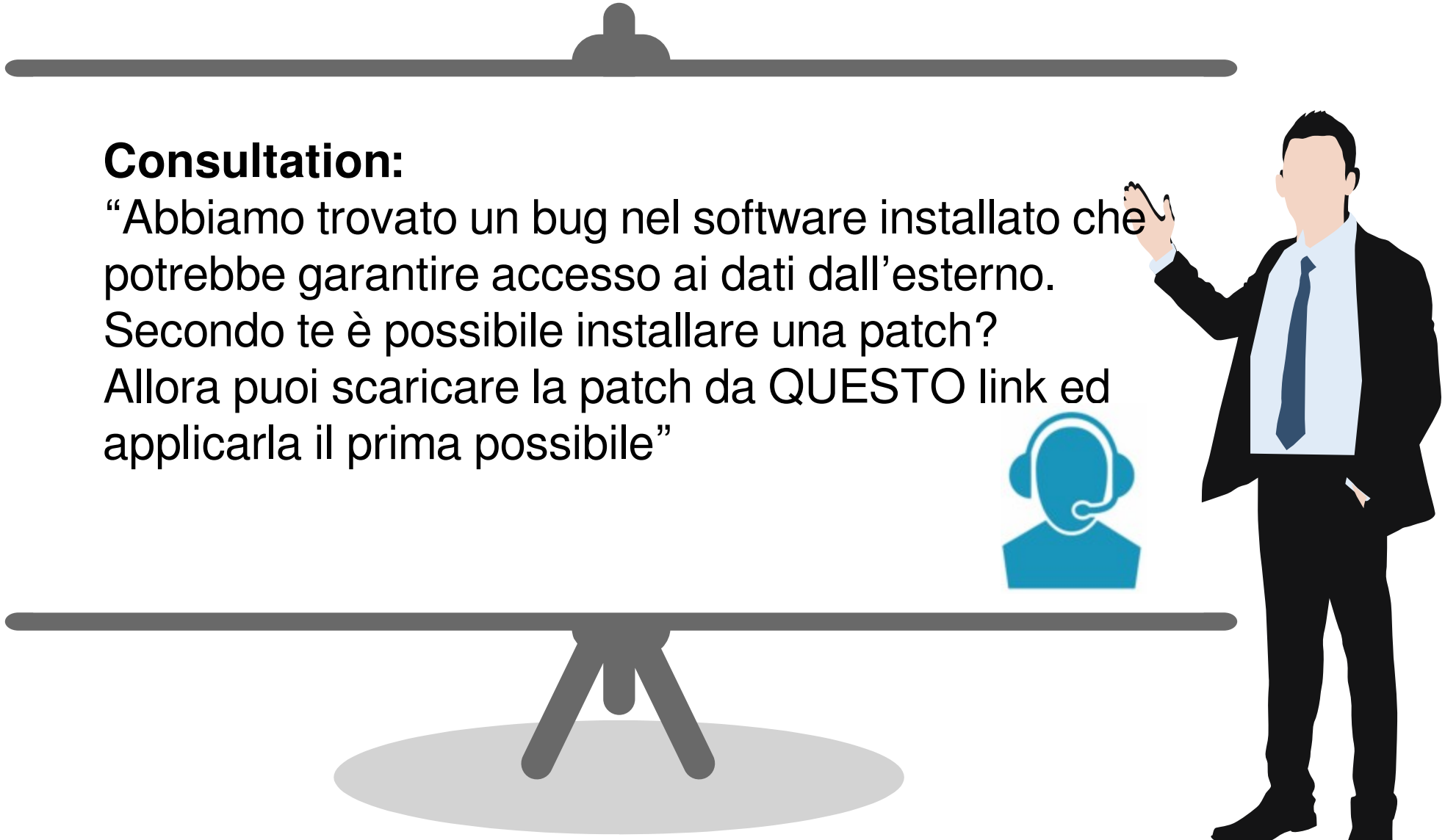
Consultation:
L’hacker tenta di coinvolgere la vittima nell’azione convincendolo che la richiesta è la cosa giusta da fare

Commitment and Consistency:
la vittima è più disponibile ad eseguire l’azione se è la cosa giusta da fare

www.presentationgo.com

Tecniche di influenza

Consultation:
“Abbiamo trovato un bug nel software installato che potrebbe garantire accesso ai dati dall’esterno. Secondo te è possibile installare una patch? Allora puoi scaricare la patch da QUESTO link ed applicarla il prima possibile”



www.presentationgo.com

Tecniche di influenza

Inspiration appeal:
“L’hacker tenta di fare leva sugli ideali della vittima per far eseguire la richiesta.

Obligation:
“la vittima è più disponibile ad eseguire l’azione se è moralmente obbligata”

www.presentationgo.com

Tecniche di influenza

Inspiration appeal:

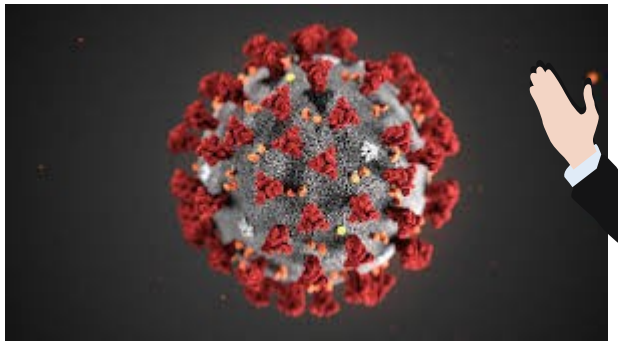
“Clicca QUI per salvare gli orsi polari dall’estinzione”

www.presentationgo.com

Tecniche di influenza

Obligation:

“Clicca qui per sapere come aiutare la tua provincia contro il COVID-19”



www.presentationgo.com

Tecniche di influenza

Curiosity:

L’hacker cerca di fare leva sulla curiorità della vittima.
La vittima è più disponibile a scoprire nuove cose.

www.presentationgo.com

Tecniche di influenza

Curiosity:

“Ciao, c’è un pacco per te!
Aprilo e scopri cosa contiene!”

www.presentationgo.com

Tecniche di influenza

Curiosity:

“Ragazzi, ho trovato una penna USB nel parcheggio con scritto -foto mare Sofia-”.

www.presentationgo.com

Tecniche di influenza

Curiosity:

“Ho ricevuto una telefonata dalla Tunisia... chissa chi è!”.

www.presentationgo.com

Tecniche di influenza

Pressure/Scarcity:

L’hacker cerca di far eseguire l’azione alla vittima mettendole fretta in modo da non farle valutare i pericoli
La vittima è più disponibile a correre dei rischi se l’offerta è allettante ma scade a breve

www.presentationgo.com

Tecniche di influenza

Pressure:

Clicca ora sul link per ottenere vantaggi esclusivi, l’offerta scade da 5 minuti.

www.presentationgo.com

Tecniche di influenza

Pretexting:

L’hacker inventa un pretesto per prendere contatto con la vittima, acqusirne la fiducia e per chiedere informazioni utili.
Impersonare un collega di una sede remota o un possibile Cliente.

www.presentationgo.com

Attacchi

www.presentationgo.com

Attacchi

- Baiting
- Vishing
- Phishing
- SpearPhishing
- Whaling
- Shoulder surfing
- Tailgating
- ...

www.presentationgo.com

Attacchi

Baiting:

Come i cavalli di troia, l’hacker lascia in luoghi
Di facile accesso supporti rimovibili con virus,
malware... ed attende che qualcuno li utilizzi

www.presentationgo.com

Attacchi

Baiting:

zanzibar	20/06/2019 12:16	Cartella di file	
DSC0824F.PNG	20/06/2019 12:16	Collegamento	3
DSC1025A.PNG	15/05/2019 15:45	Immagine PNG	327
DSC2474Z.PNG	15/05/2019 15:45	Immagine PNG	494
DSC24812F.PNG	15/05/2019 15:51	Immagine PNG	440
DSC26912J.PNG	15/05/2019 15:46	Immagine PNG	656
DSC30153R.PNG	15/05/2019 15:47	Immagine PNG	648
DSC30461S.PNG	15/05/2019 15:49	Immagine PNG	279
DSC30572P.PNG	15/05/2019 15:50	Immagine PNG	551
DSC31571M.PNG	15/05/2019 15:51	Immagine PNG	443
DSC32459Y.PNG	15/05/2019 15:52	Immagine PNG	811
DSC33476W.PNG	15/05/2019 15:53	Immagine PNG	470
DSC33814E.PNG	15/05/2019 15:44	Immagine PNG	622

www.presentationgo.com

Attacchi

Phishing:

Impersonare persone o aziende per ottenere informazioni o credenziali

- Siti web falsi di aziende famose (Poste Italiane)
- Email provenienti da aziende famose

www.presentationgo.com

Attacchi

Vishing:

Come il phishing, ma applicato ai servizi telefonici

- Servizi fasulli (Call center che chiedono il C.F.)
- Chiamate della propria banca

www.presentationgo.com

Attacchi

Whaling:

Come il phishing, ma l’obiettivo è una persona importante di un’azienda

- richiede una buona base di informazioni sull’azienda/vittima

www.presentationgo.com

Attacchi

Spear phishing:

Come il phishing, ma l’obiettivo è un gruppo ristretto di persone o una specifica compagnia

- richiede una buona base di informazioni sull’azienda/vittima

www.presentationgo.com

Attacchi

Tail gaiting:

L’hacker cerca di accodarsi ad altre persone per evitare controlli

www.presentationgo.com

Attacchi

Shoulder Surfing:

L’hacker si posiziona dietro la vittima per carpire informazioni utili.

www.presentationgo.com

Attacchi

Dumpster Divers:

L’hacker rovista nella spazzatura in cerca di informazioni utili.

www.presentationgo.com

Resoconto

Eseguire un rapporto dettagliato su:

1. Informazioni sfruttate
   (white/gray/black box, persone coinvolte)
2. Punti deboli sfruttati
3. Documenti esfiltrati
4. Remediation

www.presentationgo.com

Raccomandazioni

1. Avere sempre le autorizzazioni scritte!
2. Non pubblicizzare l'attacco né prima, né dopo
3. Descrivere minuziosamente tutte le fasi del P.T. nel rapporto conclusivo (rimane anche a voi!!)
4. Fare tesoro delle esperienze pregresse

www.presentationgo.com

Grazie!

Se ti è piaciuto questo seminario clicca QUI per aiutare i programmatori in difficoltà

www.presentationgo.com