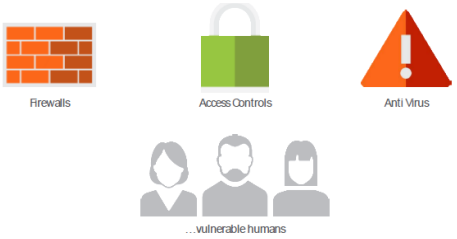
Social Engineering

Gli attacchi di ingegneria sociale sono in circolazione dagli anni ‘90, quindi il loro funzionamento è ben noto. Nonostante ciò, sono ancora una delle tecniche di attacco più utilizzate dagli attaccanti e sono una delle tecniche più pericolose. Cosa sono questi attacchi di ingegneria sociale? **Gli attacchi di ingegneria sociale comportano una manipolazione psicologica delle persone per indurle a compiere azioni** (come ad esempio cliccare sul link) **oppure a divulgare informazioni personali** (come ad esempio la password) → per questo motivo, ci riferiamo agli utenti in generale, come il Soft Center in Hard Shell, ovverosia: l’hard Shell (ovvero il guscio duro) è rappresentato da tutte le misure di protezione che vengono adottate dall’organizzazione per proteggersi dagli attacchi informatici, come ad esempio:

- l’organizzazione può installare un anti-virus per identificare se le macchine dell’organizzazione sono state infettate da un malware;
- l’organizzazione può adottare meccanismi di controllo dell’accesso ai propri servizi e/o informazioni;
- l’organizzazione può adottare firewall, i quali proteggono le connessioni di rete (bloccando, ad esempio, le connessioni provenienti da un certo indirizzo IP);

Però, dietro queste misure di protezione vi è sempre un utente, che le utilizza e che le configura ed in particolar modo, abbiamo che l’utente presenta delle vulnerabilità, le quali possono essere sfruttate dagli attaccanti per bypassare queste misure di protezione.



A sostegno di ciò, vi è una famosa fase che si dice a riguardo: “Un'azienda può spendere centinaia di migliaia di dollari in firewall, sistemi di rilevamento delle intrusioni, crittografia e altre tecnologie di sicurezza, ma se un attaccante può chiamare una persona fidata all'interno dell'azienda, e questa esegue gli ordini dell’attaccante, tutti i soldi spesi in tecnologia sono essenzialmente sprecati".

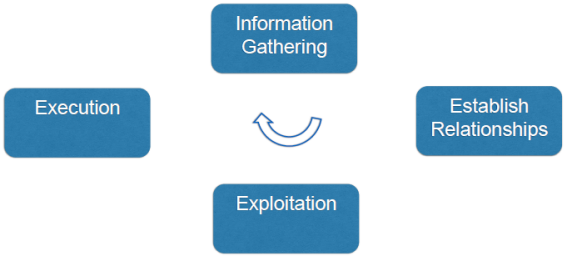
Quali sono le principali categorie di ingegneri sociali, ovverosia di attaccanti? Vi sono tre principali categorie di ingegneri sociali:

1. **Cybercriminali** → essi utilizzano le tecniche di ingegneria sociali tipicamente a scopo finanziario, in quanto l'obiettivo principale dei cybercriminali è quello di guadagnare. Quindi, i cybercriminali utilizzano le tecniche di ingegneria sociale o per effettuare dei trasferimenti di denaro illegittimi, oppure utilizzano le tecniche di ingegneria sociale per installare malware sulle macchine delle vittime e poi chiedere il riscatto, oppure per effettuare degli attacchi al DDoS;
2. **Identity Thieves** → essi sono una particolare tipologia di cybercriminali, che hanno come obiettivo quello di rubare informazioni sensibili alle vittime. Tipicamente il loro focus è di raccogliere informazioni personali, in quanto grazie a quest'ultime, gli Identity Thieves riescono a impersonale le vittime, ovverosia riescono a creare un'identità falsa con i dati di un utente vero;
3. **Scam Artists** → anche loro hanno come obiettivo quello di guadagnare e lo fanno tramite frodi condotte online tramite reti sociali (un esempio di ciò sono le romance scams oppure Facebook lottery scam).

Sorge a questo punto spontanea la domanda: Come viene condotto un attacco di ingegneria sociale? La Cyber Kill Chain di un attacco di ingegneria sociale è composta da quattro fasi principali:

1. **Information Gathering** → questa prima fase è comune a tutti gli attacchi e in tale fase, l'obiettivo è quello di raccogliere tutte le informazioni delle vittime designate. Questa fase è molto importante, soprattutto per gli attacchi di ingegneria sociale, per il successo dell'attacco, in quanto tutte le informazioni che riusciamo a raccogliere sulle potenziali vittime dell'attacco ci aiutano nella fase successiva, ovvero nella fase di Establish Relationship;
2. **Establish Relationships** → in questa fase, noi attaccanti dobbiamo contattare la vittime e stabilire una relazione di fiducia con esse e quindi, oltre a recuperare informazioni come l'indirizzo email o il ruolo che l'utente ricopre all'iterno dell'organizzazione, dobbiamo anche recuperare informazioni personali dell'utente (come ad esempio eventuali hobby) per riuscire a stabilire la relazione di fiducia;
3. **Exploitation** → in questa fase, grazie alla relazione di fiducia che si è creata con la vittime, quest'ultima viene portata a compiere l'azione che vogliamo noi come attaccanti (come ad esempio aprire un allegato, oppure resettare la password dal link dell'email);

4. **Execution** → fase finale dell'attacco, in cui gli ingegneri sociali tentano di coprire le loro tracce o comunque di chiudere la relazione che si era creata con le vittime, in modo tale da non destare sospetti.



Gli attacchi di ingegneria sociali si possono dividere in due macro-categorie:

1. Attacchi **computer based** → in quanto non richiedono la prossimità fisica con la vittima, ma possono essere condotti mediante mezzi di comunicazione. Alcuni esempi sono: phishing, spear phishing, vishing;
2. Attacchi **fisici** → in quanto essi richiedono la prossimità fisica con la vittima. Alcuni esempi sono: dumpster diving, shoulder surfing, tailgating.

Analizziamo meglio ognuno di questi attacchi e partiamo con gli attacchi computer based:

- **Phishing** → il phishing è il tentativo di acquisire informazioni sensibili come nomi utente, password e dati di carte di credito (e talvolta, indirettamente, denaro), spesso per motivi malevoli, mascherandosi come un'**entità affidabile** in una comunicazione elettronica (prevalentemente via email), in modo tale da riuscire ad accedere alla macchina delle vittime. Solitamente l'attacco non è mirato, bensì con il phishing si cerca di colpire il maggior numero di utenti;
- **Spearphishing** → particolare tipologia di attacco di phishing, condotto specificamente contro un'organizzazione o un utente bersaglio all'interno dell'organizzazione (quindi gli attaccanti devono raccogliere informazioni sull'organizzazione) e conseguentemente adattato alla vittima, utilizzando informazioni all'interno dell'email, che sono uniche per la vittima, al fine di far sembrare autentica l'email;
- **Whaling** → attacco di spearphshing, in cui l'obiettivo sono tutti i C Level Executive dell'organizzazione, ovverosia tutte le persone con un elevato grado di autorità all'interno dell'organizzazione. L'obiettivo di questo attacco, quindi, è di convincere tali utenti a compiere determinate azioni, come:
  - autorizzare trasferimenti di denaro;

    - cliccare sul link nell’email, che comporta l’installazione di malware;
    - rivelare informazioni dell’organizzazione stessa.
- **Smishing** → attacchi di phishing, che invece essere condotti via email, vengono condotti via SMS;
- **Vishing** → un’altra categoria di attacchi che sta prendendo sempre più piede e consistono nel convincere le vittime a divulgare informazioni personali (quali ad esempio le proprie credenziali d‘accesso) tramite telefono → un esempio di questo attacco, è quando l’operatore della banca chiama la vittima, dicendogli che c’è stato un problema con il suo account e quindi fornire le credenziali d’accesso all’account bancario e/o fornire l’accesso remoto alla macchina per risolvere il problema.

Passiamo ora ad analizzare le categorie di attacchi fisici, ovvero attacchi che richiedono la prossimità fisica con la vittima. I seguenti attacchi sono:

- **Dumpster Diving** → consiste nell’andare a frugare nella spazzatura dell’organizzazione target, in quanto molto spesso le password vengono scritte sui post-it, i quali successivamente vengono buttati nella spazzatura. Oppure vengono buttati documenti, come ad esempio i cedolini paga, che riportano:
    - informazioni relative ai dipendenti dell’azienda;
    - informazioni sugli ultimi meet svolti.
- **Shoulder Surfing** → tecnica di ingegneria sociale usata per ottenere informazioni come codici PIN, password ed altri dati confidenziali osservando la vittima standole alle spalle. L'attacco può venire effettuato sia da vicino (osservando direttamente la vittima) o da più lontano, usando ad esempio riprese di telecamere a circuito chiuso, binocoli o dispositivi simili. Attaccare usando questa tecnica non richiede nessuna abilità particolare; l'attenta osservazione di ciò che sta intorno alla vittima e dei movimenti da lei effettuati con la mano mentre digita un PIN sono sufficienti. I posti affollati sono quelli in cui è più facile che una vittima venga attaccata tramite shoulder surfing;
- **Tailgating** → il tailgating è una tattica che si appoggia a un dipendente, un appaltatore, un visitatore legittimo, ecc. per entrare in un edificio o in un'altra area riservata senza autorizzazione. Il tailgating è un accesso fisico non autorizzato che può causare danni alla proprietà fisica e attacchi informatici. I tailgaters utilizzano tipicamente tattiche di social engineering per ottenere un accesso non autorizzato, manipolando le caratteristiche comportamentali umane per entrare in un'area riservata. Un esempio potrebbe essere un intruso che

trasporta un carico di pacchi e poi chiede a qualcuno di tenere aperta una porta: i tailgaters sfruttano il nostro istinto di essere amichevoli e gentili. Una volta entrato in un'area riservata, il tailgater può iniziare a danneggiare la proprietà, rubare informazioni, ottenere credenziali di accesso e persino installare malware.

> 💡 L'**88%** delle organizzazioni di tutto il mondo ha subito tentativi di spear phishing nel 2019;
> Il **95%** di tutti gli attacchi alle reti aziendali sono il risultato di spear phishing riusciti;
> Il **97%** degli utenti non è in grado di identificare un'email di phishing sofisticata

Come facciamo a riconoscere l'email di phishing? Le caratteristiche comuni a queste email sono:

- **Branding Inconsistencies** → ovverosia nell'email non viene inserito alcun logo dell'organizzazione che gli attaccanti si fingono di essere. L'aspetto e/o il contenuto dell'email di phishing non è in linea con le email che si ricevono regolarmente dall'entità. Molto spesso, nelle email di phishing vi sono delle richieste inusuali all'entità;
- **Sender and Cashier** → ovverosia nell'email di phishing vi sono molti errori di battitura e di grammatica nel testo. Inoltre, molto spesso nelle email di phishing viene scritto "**Y**our account" invece di "**y**our account". Inoltre, il dominio non corrisponde all'indirizzo della persona che ci contatta ed è scritto in maniera strana;
- **Hyperlink target mismatch** → ovverosia dobbiamo verificare il link presente nell'email di phishing.

Tattiche di persuasione

Un aspetto utilizzato molto spesso dagli attaccanti sono le **tecniche di persuasione**, che massimizzano le chance che le vittime facciano quello che gli viene richiesto dall'attaccante. Alcune di queste tattiche sono:

- Il **principio di autorità** → ovverosia che solitamente l'email viene inviata da qualcuno, che ha una posizione di superiorità. Per esempio, se l'utente è un cittadino comune, l'email di phishing può impersonale un ente governativo (come ad esempio l'Agenzia delle Entrate) o la banca;

- Il **principio di scarsità** → esso sfrutta il fatto che, se una vittima pensa che una risorsa e/o un servizio sia limitatamente disponibile, allora la vittima sarà più portata a fare l'azione richiesta dall'ingegnere sociale. Solitamente, il principio di scarsità nelle email viene implementato instillato un senso di urgenza nelle vittime (come per esempio, viene richiesto alle vittime di compiere una determinata azione entro 24 ore);
- Il **principio di consistenza** → riguarda il fatto, che solitamente le persone quando compiono determinate azioni, lo fanno in maniera consistente, ovverosia mantengono sempre lo stesso comportamento e quindi si comportano in maniera coerente. Quindi, se le vittime hanno soddisfatto una volta una richiesta dell'attaccante, allora lo faranno di nuovo;
- Il **principio di liking** → secondo tale principio, abbiamo che se l'email arriva da qualcuno che la vittima conosce e/o con cui la vittima condivide degli interessi comuni, è più probabile che la vittima compia le azioni volute dall'attaccante;
- Il **principio di reciprocità** → esso sfrutta il fatto, che se l'attaccante offre un determinato servizio alla vittima, molto probabilmente quest'ultima sarà disposta a fare qualcosa in cambio. Per esempio, l'attaccante si finge un'organizzazione che vende prodotti biologici e nell'email sostiene che, se la vittima compila un questionario per scopi commerciali, l'azienda gli darà un voucher di 20$;
- Il **principio del Social Proof** → esso sfrutta il fatto, che le vittime tendono a fare quello che la maggior parte delle persone fa. Quindi, se l'attaccante all'interno dell'email dice che altre persone hanno fatto l'azione che richiede, più probabilmente la vittima farà l'azione.

Sorge spontanea la domanda: **Quale tattica di persuasione è più efficace?** Non ci sono molti studi a riguardo, quello che però si è scoperto, da diversi studi sull'analisi delle email, **i principi maggiormente utilizzati sono quello di autorità e quello di scarsità**.

Phishing Websites

I siti di phishing godono di alcune caratteristiche:

- Nomi di dominio irregolari → il nome del dominio è diverso rispetto a quello del sito originale e può presentare delle discrepanze con il contenuto stesso

del sito. Per esempio, il dominio può essere francese, ma il sito è scritto in tedesco;

- Manca il protocollo HTTPS nell'URL → quindi non utilizzano una connessione cifrata;
- Registrano sotto il dominio corretto un sotto-dominio, che in realtà punta al sito di phishing;

In realtà, al giorno d'oggi, **avere una connessione sicura non è più sintomo di garanzia che il sito non sia un sito di phishing** → questo perchè i phisher vanno ad utilizzare sempre più servizi cloud (quali ad esempio Google, Dropbox e Microsoft) per ospitare i propri siti di phishing. Il vantaggio di questo approccio è che il dominio del sito contiene il riferimento a Windows.NET, che quindi quando viene visualizzato dalle vittime sembra legittimo e infatti se si utilizza il comando UISP, per controllare il certificato associato al dominio, ci verrà detto che il certificato è stato rilasciato da Microsoft.

Un'altra tattica utilizzata dai phisher è quella di **ospitare il proprio sito di phishing all'interno di altri siti legittimi** → ovvero abbiamo, che i social engineer vanno ad individuare quei siti che sono stati sviluppati con WordPress e una volta fatto ciò, vanno ad ottenere l'accesso alla console di amministratore di WordPress mediante attacchi di brute force o di phishing. Si connettono alla console e questo punto possono modificare il sito in WordPress, installano dei plugin ed infine vanno a reindirizzare le vittime alla pagina realizzata con WordPress, utilizzando semplicemente gli strumenti di URL shorteling (ovvero gli strumenti che rendono più corto l'URL).

→ un'altra tecnica è quella di utilizzare l'**AI generativa**, al fine di creare: immagini, video, email di phishing, ricreare delle voci o addirittura ologrammi.

Come i malware e i ransomware si sono evoluti in un'organizzazione As a Service, anche il phishing si è evoluta in questa direzione → ci sono pacchetti/framework che aiutano i social engineer a condurre attacchi di phishing. In particolare, uno dei framework utilizzati maggiormente durante le campagne di phishing di quest'anno è **EvilProxy** → esso può essere affittato pagando un abbonamento mensile e quello che ci fornisce è un portale, tramite il quale possiamo configurare la nostra campagna di phishing. L'utilizzo che viene fatto principalmente di questo framework, è per compromettere l'autenticazione a due fattori, utilizzando una tecnica chiamata Reverse Proxy → questa tecnica funziona nel seguente modo: il reverse proxy è un proxy che sta tra l'utente legittimo e il sito presso il quale l'utente deve autenticarsi con due fattori. Abbiamo che inizialmente l'utente fornisce il suo nome utente e la

sua password e il reverse proxy non fa altro che trasferire la richiesta di autenticazione al sito legittimo. A questo punto il sito legittimo richiede il secondo fattore di autenticazione (OTP) e il sito di phishing non fa altro che far visualizzare alla vittima l'interfaccia che ha rimandato il sito legittimo e naturalmente ila vittima inserisce il secondo fattore di autenticazione. A questo punto, quest'ultimo viene trasferito al sito legittimo e a questo punto il sito legittimo rilascerà un session cookie, che attesta che l'utente è stato autenticato con successo. Questo session cookie viene preso l'attaccante e quindi l'attaccante riesce ad autenticarsi.

→ uno strumento per identificare i siti i phishing è **PhishTank** → permette di controllare se un URL sospetto è un sito di phishing oppure no.

→ Come fa un'organizzazione a prevenire questi attacchi di phishing? Oltre all'abilità del singolo utente a riconoscere l'email di phishing attraverso degli insegnamenti/training personalizzati per ogni utente, l'azienda deve adottare delle altre misure di protezione organizzate e tecniche, che possono prevenire gli attacchi di phishing e conseguentemente adottare un **approccio a più livelli**: