Ordine degli Avvocati di Alessandria

2 Dicembre 2022

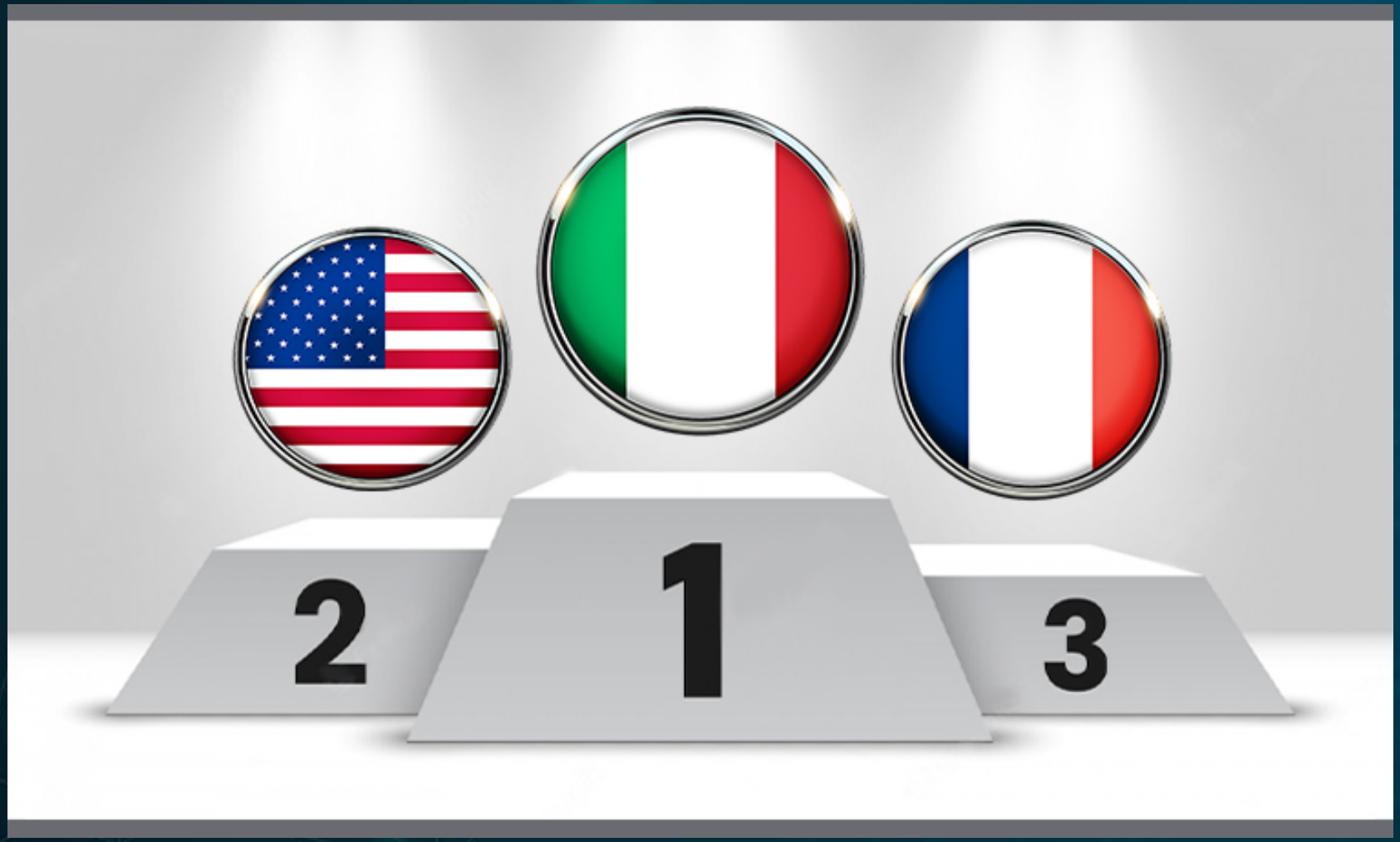
CYBER SECURITY: CASI PRATICI E PROFILI GIURIDICI

Rizzetto Michele

CEO e CYBER Security Manager di B4web S.r.l.

Indice degli Argomenti

IL PODIO DEGLI ATTACCHI



IL PODIO DELLA CARENZA CULTURALE

Le Principali Obiezioni

CYBER RISK: SCENARIO REALE

La nuova frontiera del crimine è l'attacco informatico.

Nell'ultimo anno detti attacchi sono aumentati del 246%.

Le persone indagate sono aumentate del 78%.

1 attacco ogni 39”

Ordine degli Avvocati di Alessandria

Secondo le stime del Clusit

Associazione Italiana per la Sicurezza Informatica

156 attacchi gravi al mese

Il valore più elevato mai registrato sino ad oggi

IN TUTTI GLI ATTACCHI

95%

Dovuto ad Errore Umano

Ordine degli Avvocati di Alessandria

SECONDO LE STIME DEL CLUSIT

56 %

Gli attacchi rilevati e andati a buon fine hanno avuto un impatto **ALTO e CRITICO**

28 %

ha dovuto affrontare **spese non pianificate** per correggere le lacune di sicurezza

11 %

ha dovuto **pagare** multe per la mancanza di conformità alle norme

8 %

ritiene di aver **perso** il proprio **vantaggio competitivo**

CYBER ATTACK - PUNTI DEBOLI

76% DURANTE IL WEEKEND

77% AZIENDE SENZA UN PIANO DI DIFESA E RISPOSTA AGLI INCIDENTI

83% DOVUTA AD IMPREPARAZIONE DEL PERSONALE

46% IT CHE INIZIANO AD IGNORARE GLI ALLARMI PER TROPPI FALSI POSITIVI

Tipologie di attacchi che affronteremo

Caso 1 – RANSOMWARE

Caso 2 - MAN IN THE MIDDLE

Caso 3 - PHISHING

CASO 1 - Ransomware

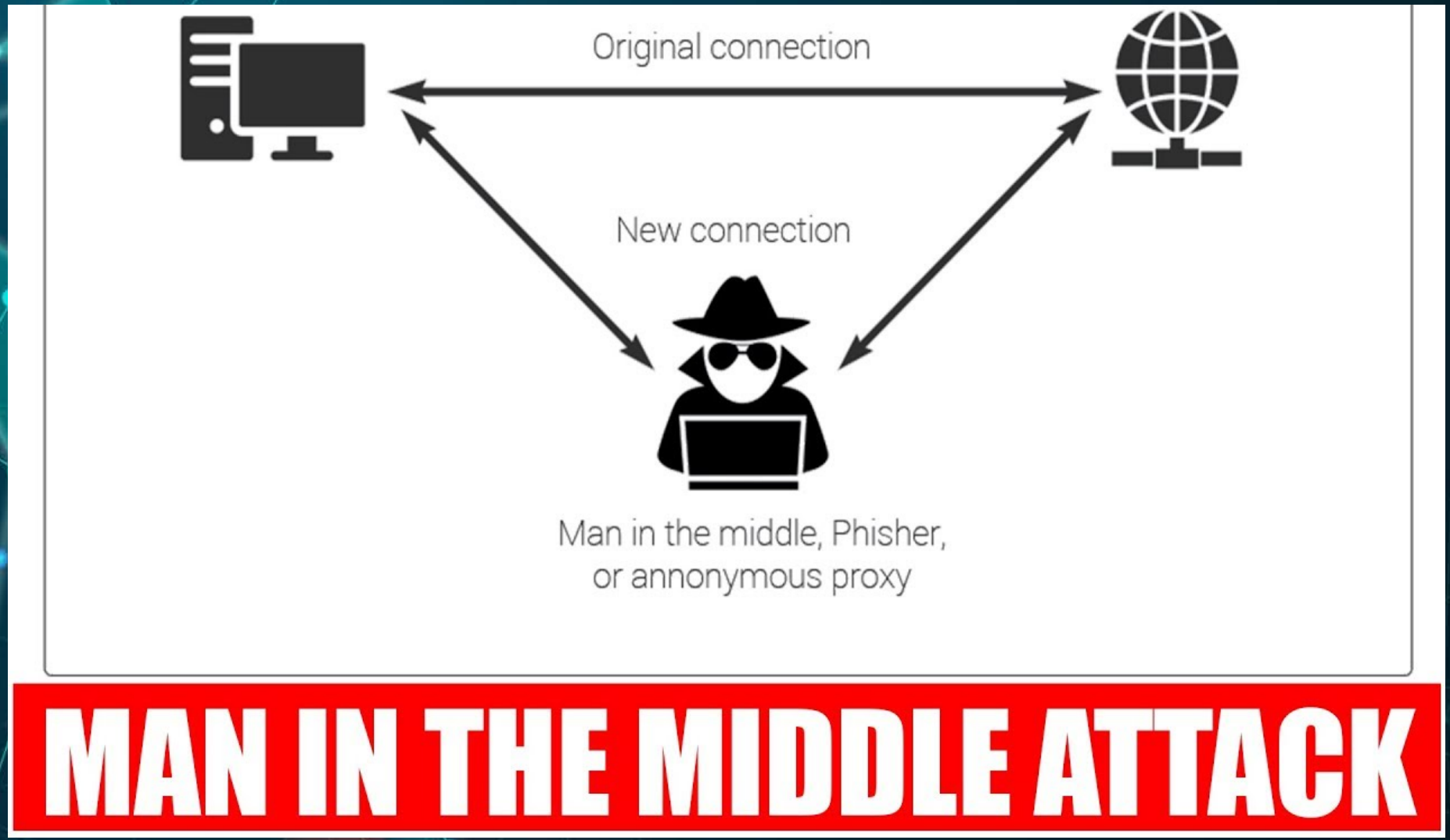
COME AVVIENE IL PAGAMENTO

OLTRE IL 60% DELLE VITTIME HA PAGATO MA «NON HA MAI RECUPERATO I PROPRI FILE»

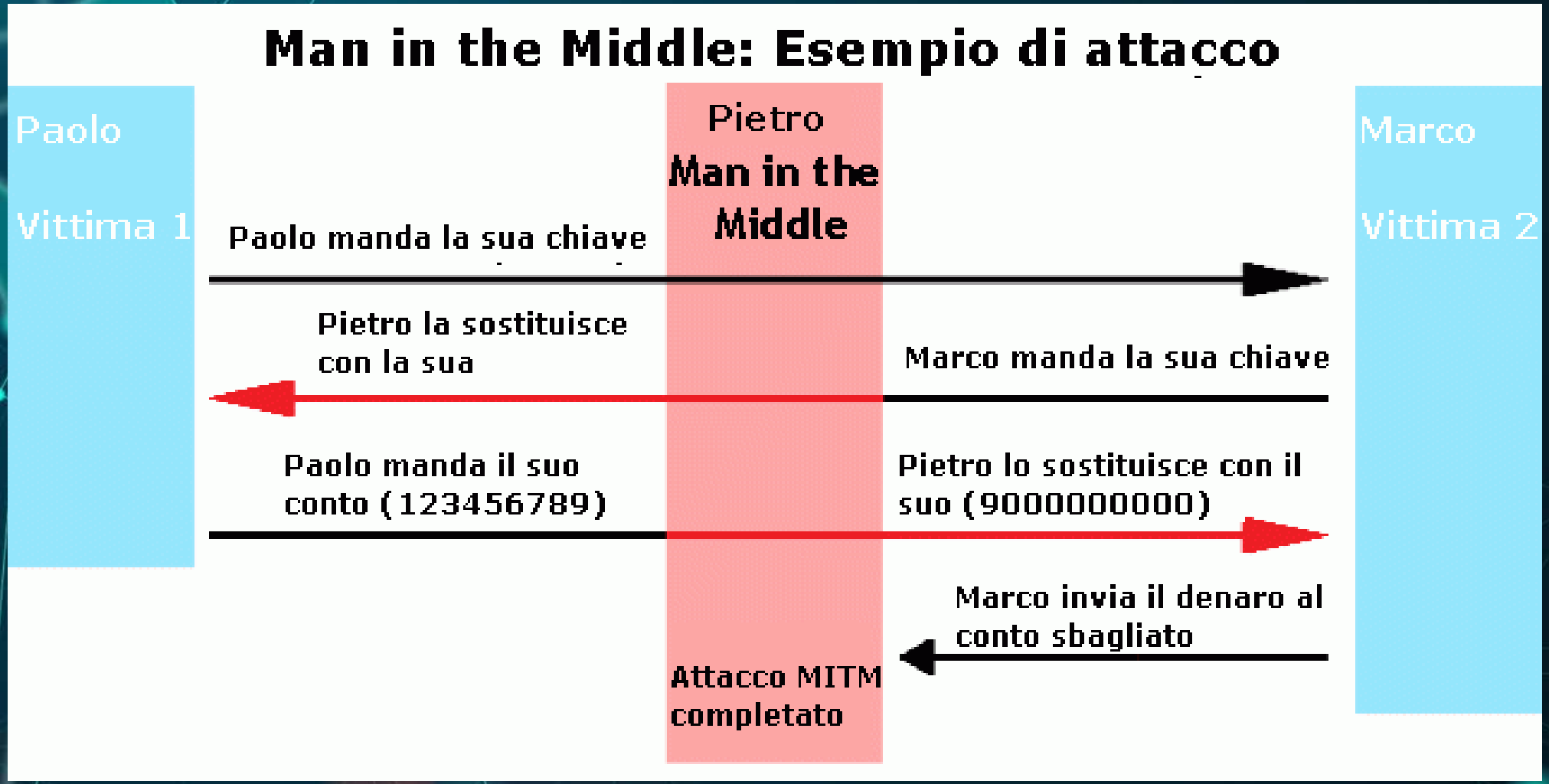
Inoltre i malcapitati che hanno scelto di pagare un RISCATTO,

l'80% ha subito un altro ATTACCO

CASO 2 - Man in the Middle

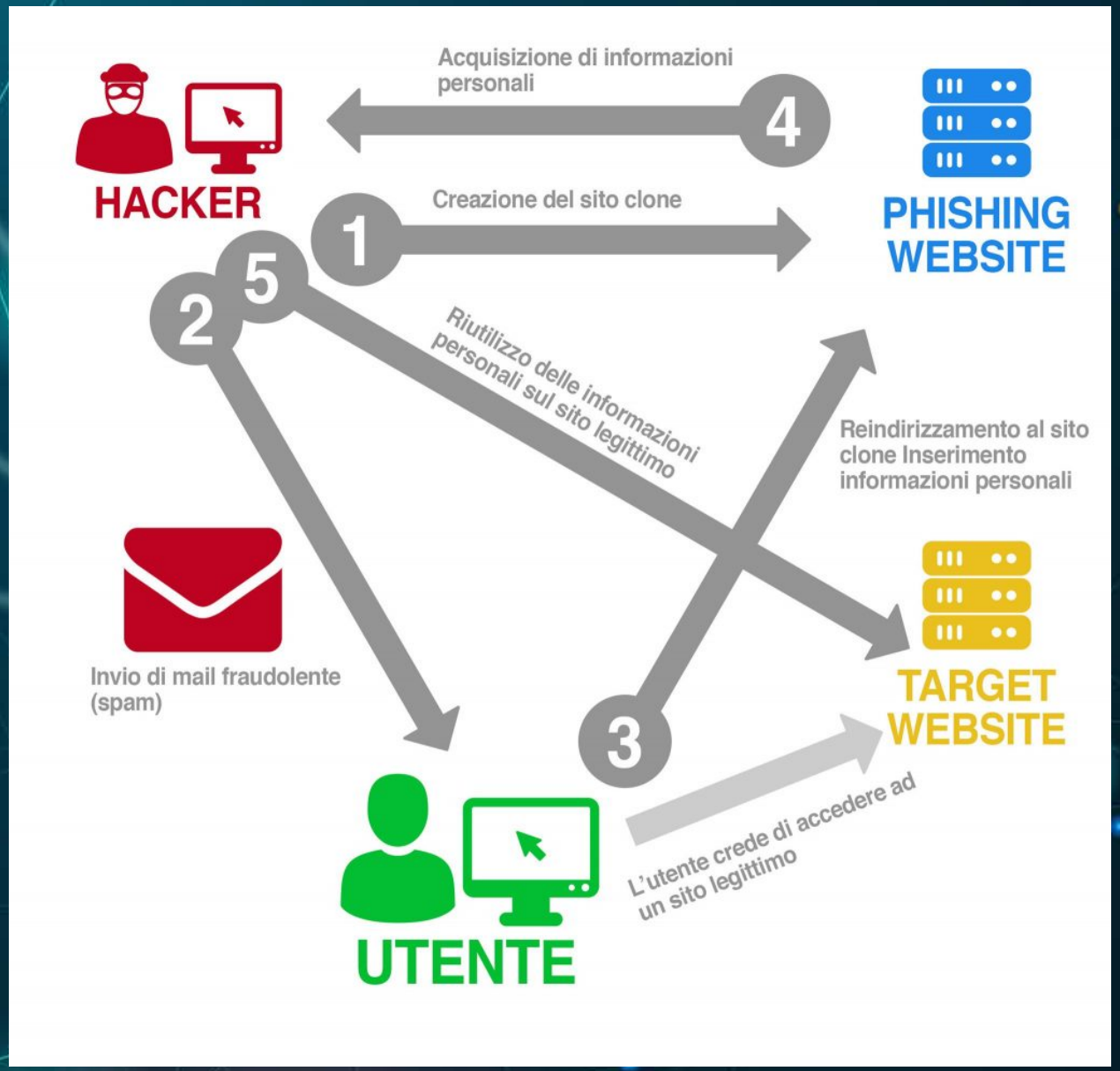


CASO 2 - Man in the Middle



COME AVVIENE IL PAGAMENTO

CASO 3 - PHISHING



Ordine degli Avvocati di Alessandria

METODOLOGIA DI ATTACCO

1. Il malintenzionato (Phisher) crea un sito clone apparentemente simile al sito ufficiale, spedisce e-Mail che simulano, nella grafica e nel contenuto quello di una istituzione nota al destinatario. (Banca, Corriere, Provider, Polizia, ecc.)

2. L'e-Mail contiene sempre avvisi particolari o problemi con C/C, Account, Pagamenti, Rimborsi, ecc.

3. L'E-mail invita il destinatario a seguire un Link per evitare addebiti, regolarizzare la sua posizione con l'ENTE o la Società di cui il messaggio simula la grafica e l'impostazione.

4. Il Link fornito non porta in realtà al Sito Ufficiale ma al sito clone apparentemente simile al sito ufficiale, ma sul server controllato dal Phisher, dove verranno chiesti alla vittima i dati personali, normalmente con la scusa di una conferma o la necessità di effettuare un'autenticazione al sistema, un pagamento, queste informazioni vengono memorizzate sul server gestito dal Phisher.

5. **È la fine: il Phisher utilizzerà questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.**

DEFINIZIONE DI PHISHING

1. Si tratta di un’attività illegale che sfrutta una tecnica di ingegneria sociale (lo studio dei comportamenti delle persone allo scopo di influenzarli):
2. Invio di messaggi fraudolenti. Nella maggior parte dei casi è una truffa tentata attraverso la posta elettronica, ma non mancano casi che sfruttano altri mezzi, come SMS

SMISHING

O tramite telefonate

VISHING

IL SOCIAL ENGINEERING…….ESISTE DA SEMPRE

È social engineering Totò che cerca di vendere la Fontana di Trevi agli americani…

Il CYBER Crime del futuro

I Protocolli PLC, HMI e SCADA

sono il cuore dell'**Industria 4.0,** ed è per questo che

stanno diventando un bersaglio allettante per gli hacker.

Ordine degli Avvocati di Alessandria

Obiettivi della Cyber Security

Disponibilità dei dati	→	Riducendo i rischi
Integrità dei dati	→	Assicurando i servizi
Tutelare i dati	→	Per la riservatezza

La SICUREZZA AL 100% non ESISTE

Un ringraziamento particolare a Ordine degli Avvocati di Alessandria per l'interesse dimostrato sull'argomento

GRAZIE PER L'ATTENZIONE

Rizzetto Michele