Phishing

Come riconoscere
email di Phishing

STRUTTURA DEL CORSO

Il corso è suddiviso in 5 parti e prevede una simulazione interattiva per riconoscere email reali di Phishing / Spam.

1

Introduzione

Contesto e definizioni.

2

Tipologie

Principali tipologie di Phishing.

3

Identificare

Come riconoscere il Phishing. Cosa fare se siamo vittime di Phishing

4

Esempi

Esempi di email di Phishing.

5

Test finale

Simulazione interattiva di email di Phishing.

INTRODUZIONE

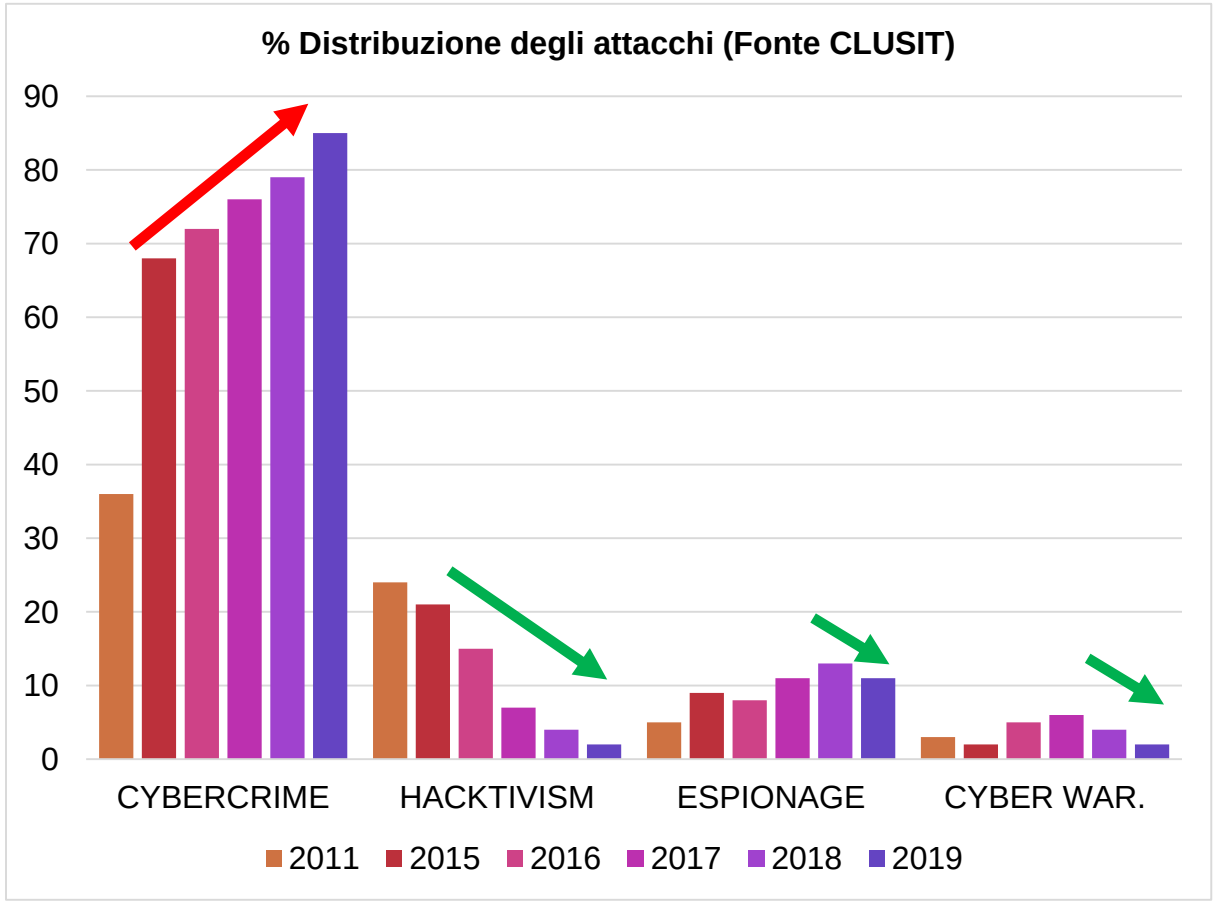
- Contesto delle minacce informatiche
- Perché è importante riconoscere il Phishing
- Definizioni

INTRODUZIONE (1/3)

Il **Phishing** è considerata una **minaccia** informatica molto rilevante, poiché utilizzata dalla maggior parte degli «attaccanti». È possibile classificare gli attaccanti in base al loro obiettivo, di seguito le principali tipologie:

- **Cybercrime** (criminali informatici)
- **Hacktivism** (attivisti)
- **Espionage** (spionaggio industriale)
- **Cyber warfare** (guerra cibernetica tra gruppi)

Negli ultimi anni si è osservato un aumento di attacchi di tipo «Cybercrime» a discapito delle altre tipologie.



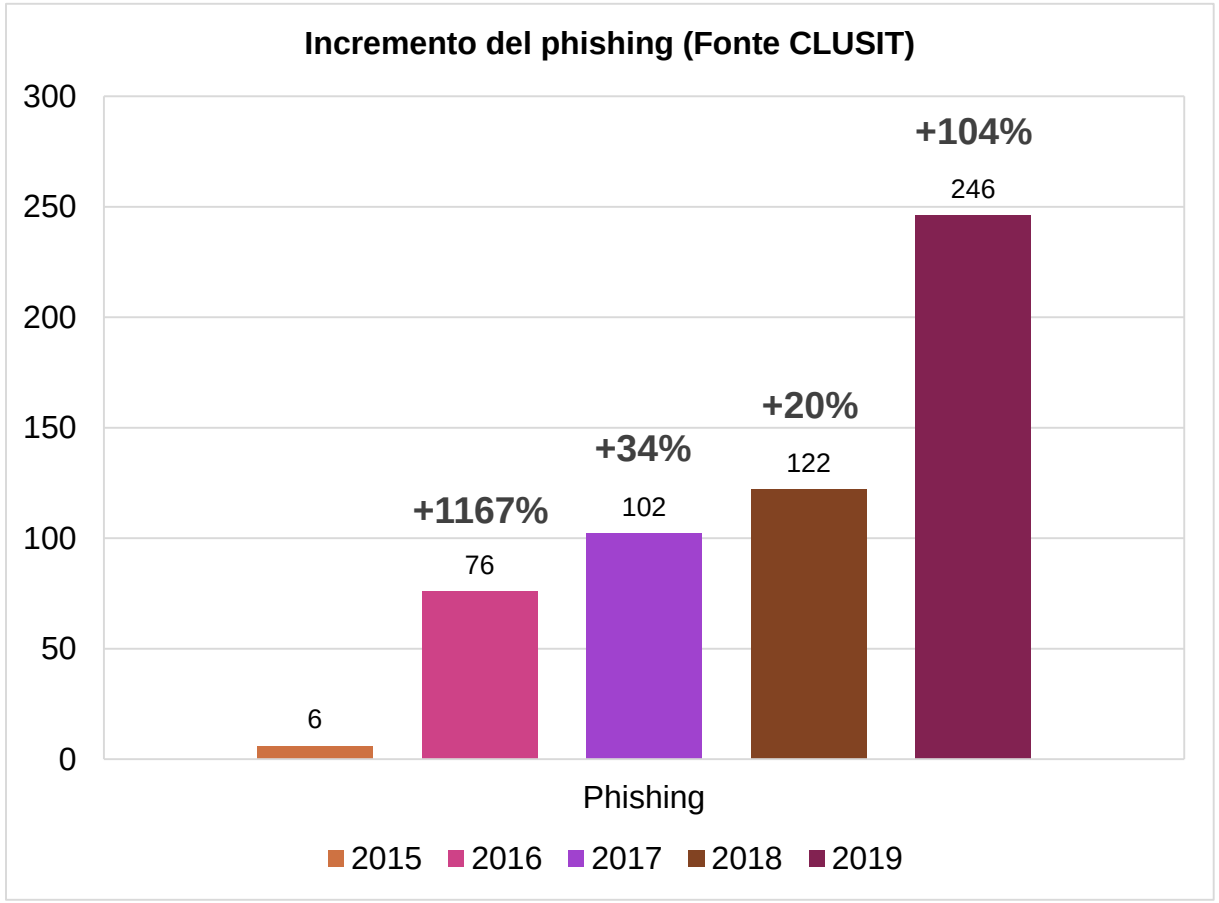
INTRODUZIONE (2/3)

Perché riconoscere il Phishing è così importante?

- Più del **90%** degli **attacchi** informatici, oggi, **inizia** con una **mail di Phishing**.
- Il **Phishing** è in **continua crescita.**

Come possiamo notare questa minaccia è in continua crescita nonostante un incremento di circa +1167% registrato nel 2016.

Questi due fattori ci portano a classificare il Phishing come un **rischio alto** a cui tutti noi siamo esposti.



INTRODUZIONE (3/3)

Definizioni

Con il termine **Phishing** (parola ricavata dai vocaboli inglesi fishing – pesca e password) si indica una particolare tipologia di **frode** telematica **via email** con lo **scopo** di **rubare dati** personali e confidenziali degli utenti. Più precisamente, attraverso il Phishing viene praticato il **furto** di credenziali (es. password), dei numeri relativi a carte di credito e conti bancari, così come ulteriori dati riservati (anche informazioni come la firma in calce all'email).

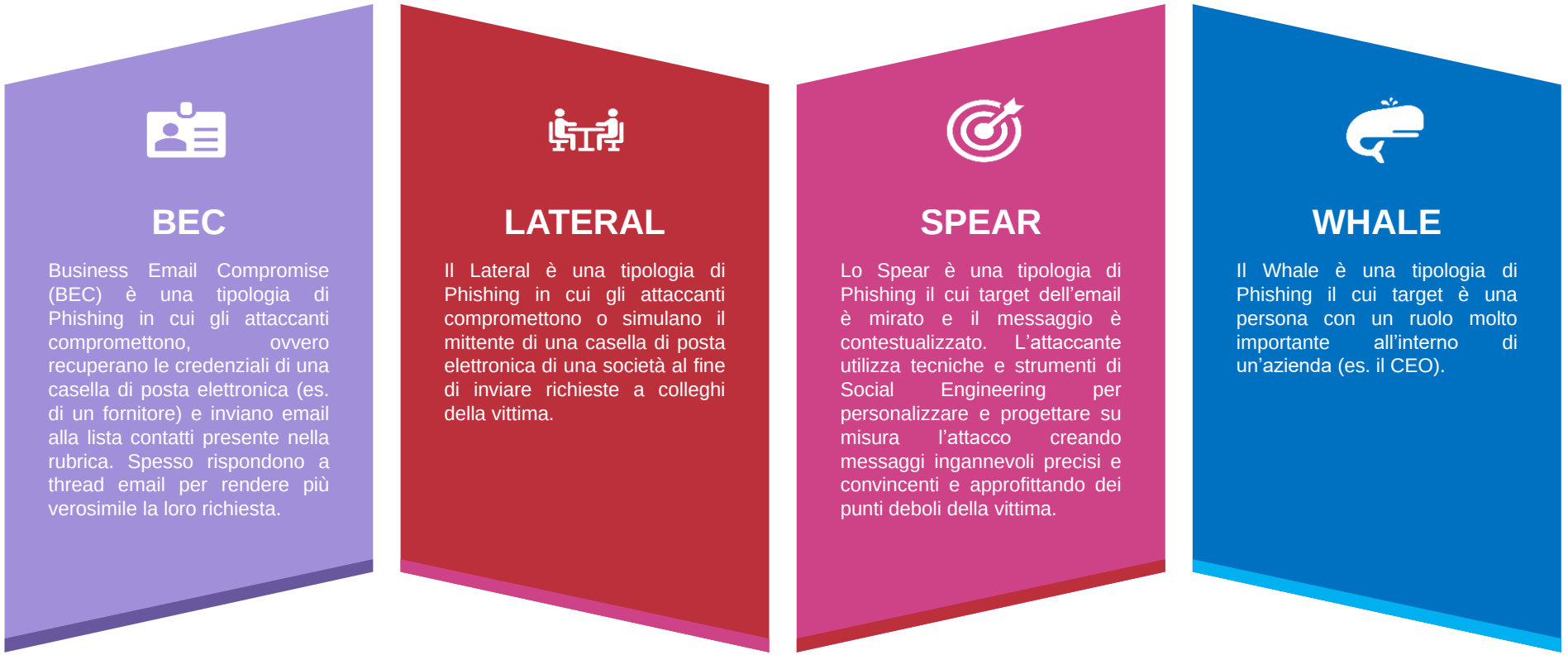
Con il termine **Spam** si indica una tipologia di email ricevuta senza che l'utente abbia espresso il proprio consenso alla ricezione dello stesso (es. campagne marketing, catene di Sant'Antonio, ecc.).

TIPOLOGIE

- Principali tipologie di Phishing

TIPOLOGIE

Le tipologie di Phishing si differenziano per tipologia di **target** (ovvero destinatario) e tipologia di **mittente** interpretato.



BEC

Business Email Compromise (BEC) è una tipologia di Phishing in cui gli attaccanti compromettono, ovvero recuperano le credenziali di una casella di posta elettronica (es. di un fornitore) e inviano email alla lista contatti presente nella rubrica. Spesso rispondono a thread email per rendere più verosimile la loro richiesta.

LATERAL

Il Lateral è una tipologia di Phishing in cui gli attaccanti compromettono o simulano il mittente di una casella di posta elettronica di una società al fine di inviare richieste a colleghi della vittima.

SPEAR

Lo Spear è una tipologia di Phishing il cui target dell'email è mirato e il messaggio è contestualizzato. L'attaccante utilizza tecniche e strumenti di Social Engineering per personalizzare e progettare su misura l'attacco creando messaggi ingannevoli precisi e convincenti e approfittando dei punti deboli della vittima.

WHALE

Il Whale è una tipologia di Phishing il cui target è una persona con un ruolo molto importante all'interno di un'azienda (es. il CEO).

IDENTIFICARE

- Come riconoscere un’email di Phishing
- Cosa fare se siamo state vittime di Phishing

IDENTIFICARE (1/2)

Un’email di Phishing è caratterizzata da alcuni elementi. Rimane sempre valido l’istinto, se il testo dell’email insinua in noi un dubbio, è fondamentale assicurarci dell’autenticità dell’email contattando il mittente (es. chiamandolo al telefono).

Mittente sospetto

Il mittente presenta un nome non coerente con l’indirizzo email, es. “da: Mario Rossi <infoACME@ACME.it>”.

Intestazione generica

Utilizzo di intestazioni come “Caro cliente” oppure utilizzo del nome email “Gentile mario.rossi”.

Link ingannevoli

I link presentano incoerenza rispetto al dominio di destinazione (passare il mouse sopra al link senza cliccare per visualizzare la destinazione).

Contenuto sospetto

Contenuto non inerente alle attività svolte nell’ambito lavorativo o personale.

Errori grammaticali

L’oggetto e il testo dell’email presentano errori grammaticali.

Allegati sospetti

Invio di file compressi “.zip” contenenti file Office, PDF di piccole dimensioni. I file di Office potrebbero chiedere attivazioni di macro malevole.

Carattere di urgenza

La presenza di un carattere di urgenza spesso legata a temi di carattere amministrativo, legali, ecc. con scadenze ravvicinate.

Stile sospetto

Utilizzo di vocaboli non appropriati o non consoni al mittente.

IDENTIFICARE (2/2)

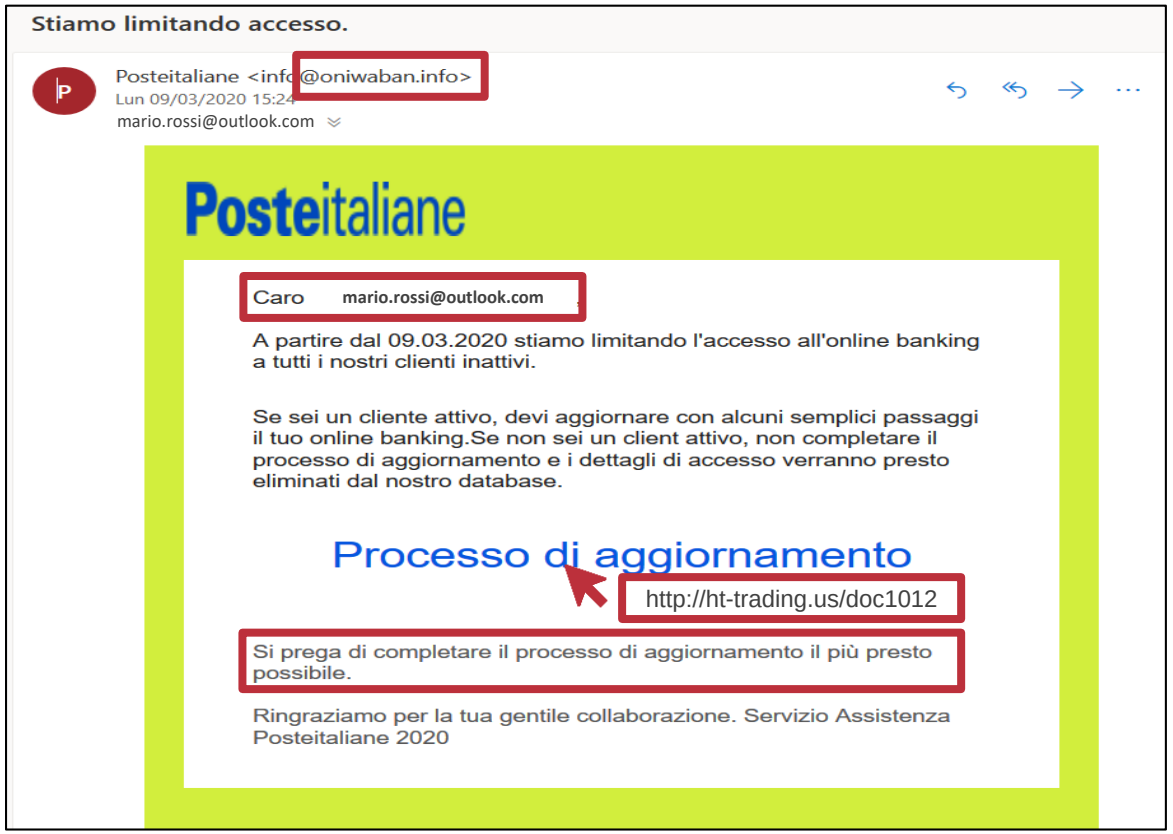
Se si sospetta di essere vittima di phishing è importante seguire alcune azioni:

- Qualora si fossero fornite credenziali è importante procedere con il cambio password il prima possibile da un computer che reputiamo pulito, ovvero privo di virus.
- Qualora si fosse scaricato un file allegato o cliccato su un link è importante aggiornare il software antivirus ed avviare subito una scansione del computer.
- Qualora si fossero inviate informazioni come: carta d'identità, numero della carta di credito, ecc. È importante procedere quanto prima alla remissione di nuovi documenti o bloccare carte, bancomat.
- Informare le autorità competenti. È fondamentale segnalare l'accaduto alle autorità competenti, come la Polizia Postale.
- Avvisare gli enti colpiti. È opportuno segnalare l'attacco phishing agli enti che ne sono stati colpiti, cosicché possano prendere provvedimenti e contrastare la truffa.

ESEMPI

- Esempi di email di Phishing

ESEMPI (1/3)



From: Posteitaliane <info@oniwaban.info>

To: mario.rossi@outlook.com

Elementi sospetti:

- Il mittente non è «@poste.it» ma un sito sconosciuto
- «Caro mario.rossi@outlook.com», utilizza un'intestazione sospetta
- Link sospetto, non è il sito ufficiale
- «il più presto possibile», carattere di urgenza

ESEMPI (2/3)

Salve!

Come avrai gia' indovinato, il tuo indirizzo email e' stato hackerato, perche' e' da li' che ho inviato questo messaggio. :(

Io rappresento un gruppo internazionale famoso di hacker.
Nel periodo dal 22.07.2018 al 14.09.2018, su uno dei siti per adulti che hai visitato, hai preso un virus che avevamo creato noi.
In questo momento noi abbiamo accesso a tutta la tua corrispondenza, reti sociali, messenger.
Anzi, abbiamo i dump completi di questo tipo di informazioni.

Siamo al corrente di tutti i tuoi "piccoli e grossi segreti", si si... Sembra che tu abbia tutta una vita segreta.
Abbiamo visto e registrato come ti sei divertito visitando siti per adulti... Dio mio, che gusti, che passioni tu hai... :)

Ma la cosa ancora piu' interessante e' che periodicamente ti abbiamo registrato con la web cam del tuo dispositivo, sincronizzando la registrazione con quello che stavi guardando! Non credo che tu voglia che tutti i tuoi segreti vedano i tuoi amici, la tua famiglia e soprattutto la tua persona pi�� vicina.

From: supermario2000@gmail.com

To: supermario2000@gmail.com

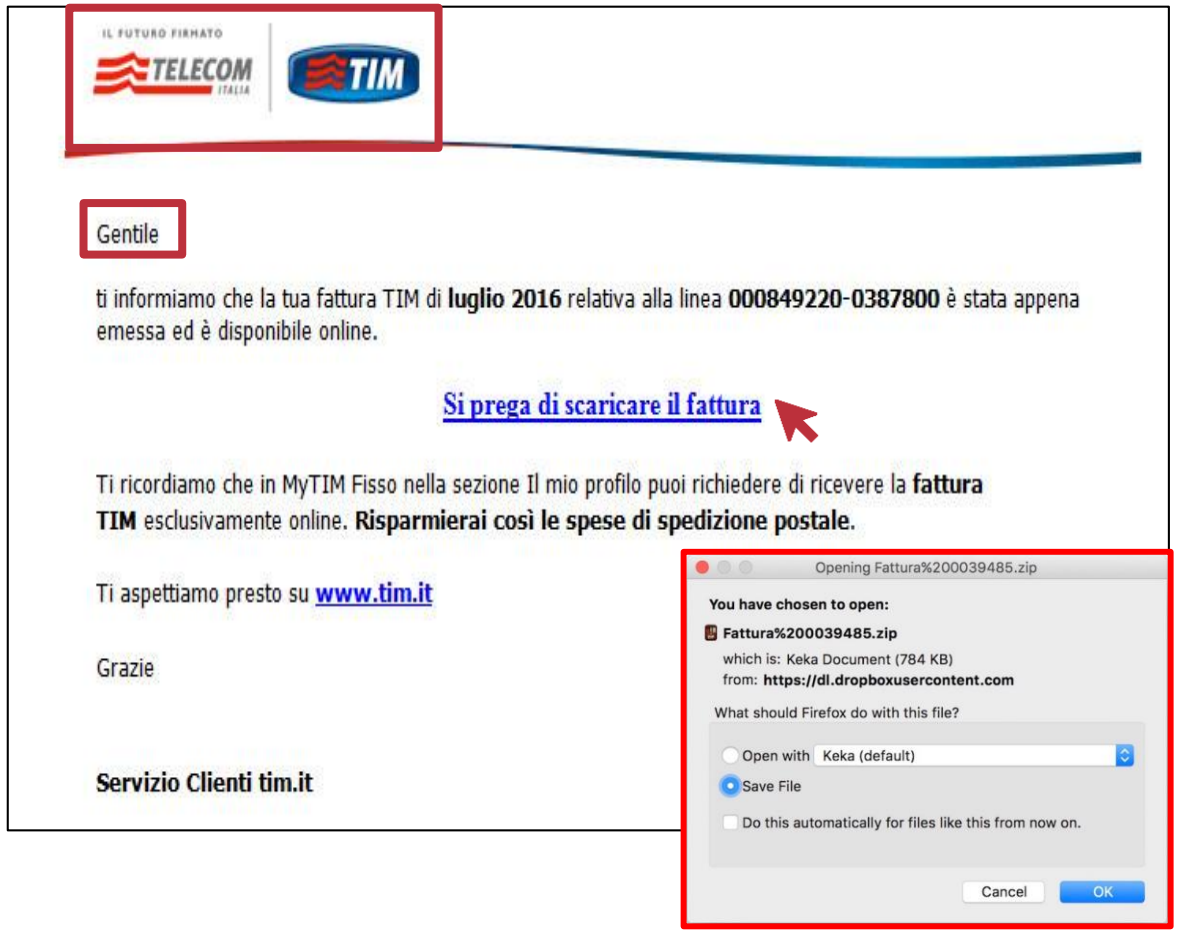
Elementi sospetti:

- «Salve!», se l'attaccante avesse davvero accesso alla nostra email conoscerebbe il nostro nome!
- Il vero mittente (è visibile solo nel sorgente email e richiede una conoscenza più tecnica)

L'attaccante utilizza la tecnica di «email spoofing» al fine di modificare il mittente.

Il campo from (da) visibile, può <u>sempre</u> essere modificato da un attaccante!

ESEMPI (3/3)



From: TIM <info@tim.it>

To: mario.rossi@gmail.com

Elementi sospetti:

- Logo non aggiornato
- «Gentile», utilizza intestazione generica
- La fattura è in formato .zip proveniente da un sito non ufficiale TIM (dropbox)
- Il vero mittente (è visibile solo nel sorgente email e richiede una conoscenza più tecnica)

TEST FINALE

- Simulazione interattiva di email di Phishing.

TEST FINALE

Per accedere alla simulazione di Phishing interattiva cliccare sul bottone «**Inizia il test**».

Il test è:

- gratuito
- non richiede registrazione
- non registra le valutazioni
- nessuna pubblicità

CREDITS

Grazie a tutti i coloro hanno contribuito e supportato il progetto.

Audio:

Google coud text-to-speech

Definizioni:

- Kaspersky Glossary

Images:

- Cover - Image by Muhammad Ribkhan from Pixabay
- Introduzione - Image by Tumisu from Pixabay
- Definizioni - Image by talha khalil from Pixabay
- Esempi - Image by gabrielle_cc from Pixabay