IL PHISHING

Alcune nozioni base su questa tecnica di attacco

Generalità

- **Phishing generale**: Il phishing è una tecnica di attacco per rubare informazioni personali.
- **Reconnaissance**: Raccolta di informazioni per creare messaggi di phishing mirati.
- **Spam phishing**: Email fraudolente per rubare dati personali, spesso usando ingegneria sociale.
- **Social Engineering**: Tecniche per convincere le vittime a rivelare informazioni riservate.
- **Whaling**: Phishing mirato a dirigenti per rubare dati aziendali e personali.

PHISHING DI SPAM (PUBBLICITA')

- Il phishing di spam è una forma di truffa online in cui i cyber-criminali inviano e-mail fraudolente per rubare informazioni personali.
- Il phishing di spam spesso utilizza tecniche di ingegneria sociale per convincere le vittime a fare clic su link o scaricare allegati dannosi.
- Le e-mail di phishing di spam possono sembrare provenire da fonti legittime, come banche, società di carte di credito o siti di shopping online.
- Le misure di sicurezza come software antivirus e la verifica dell'URL di destinazione possono aiutare a prevenire il phishing di spam.

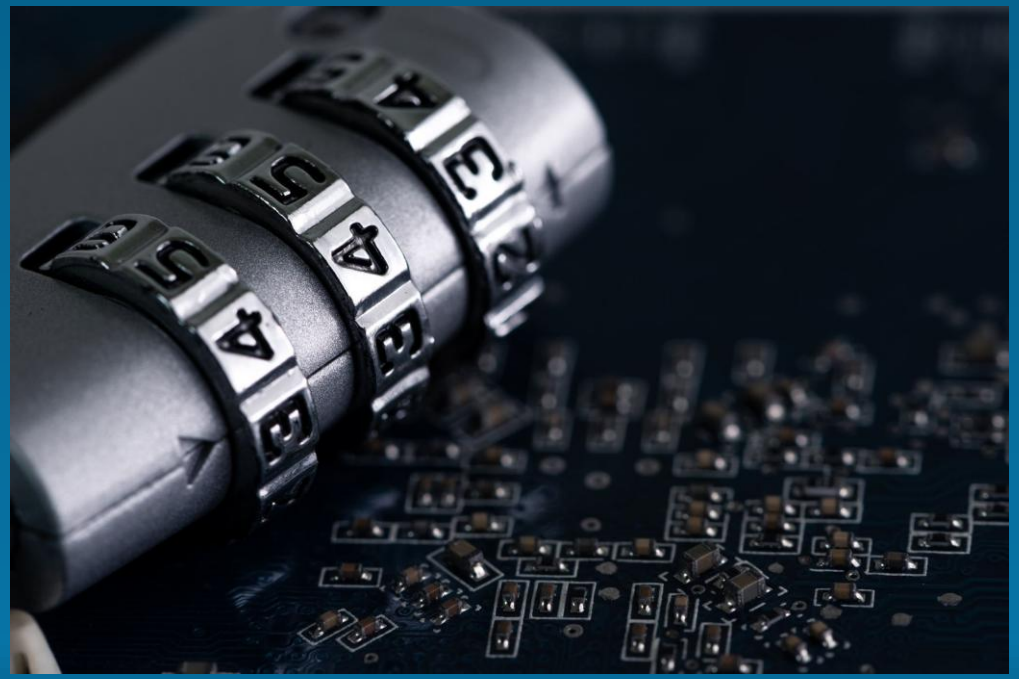
EMAIL SPAM VISHING E SMISHING

- L'email spam Vishing è una forma di phishing in cui i criminali informatici fanno leva sulle emozioni delle vittime per rubare informazioni sensibili come numeri di carta di credito e password.
- L'email spam Smishing è una forma di phishing che coinvolge messaggi di testo invece che messaggi email. I criminali informatici cercano di ingannare le vittime per rubare informazioni personali e finanziarie.
- Le tecniche di prevenzione includono la verifica dell'URL del sito web, l'installazione di software antivirus affidabile e l'educazione sui metodi di phishing comuni.

Smishing

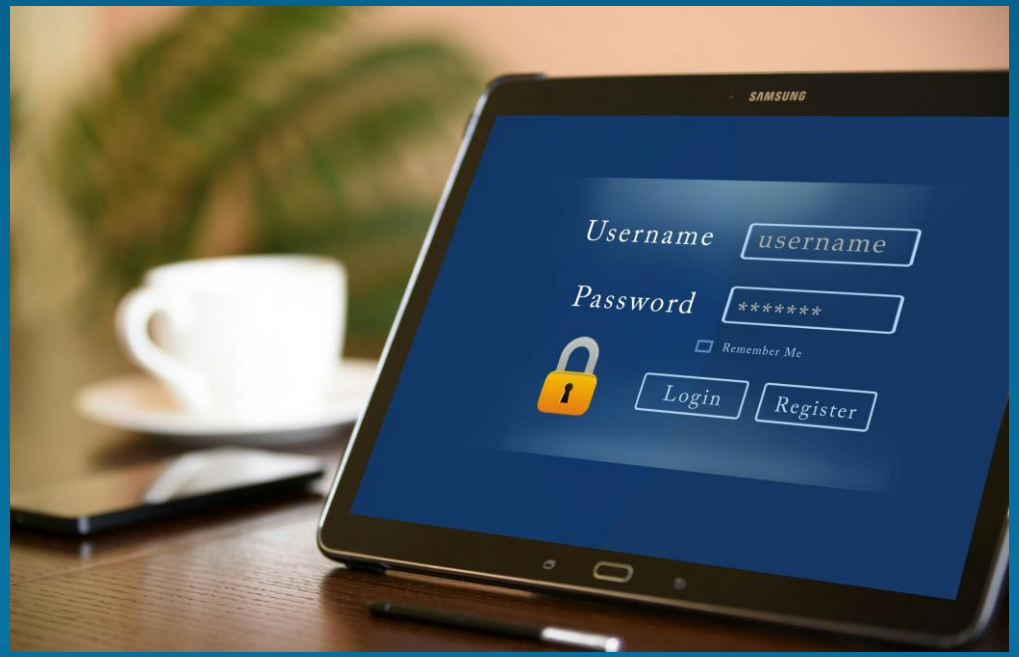
1. **Definizione**: Lo smishing è una truffa che combina SMS e phishing, dove i truffatori inviano messaggi di testo fingendo di essere enti affidabili per ottenere informazioni personali e finanziarie[1].
2. **Modalità di attacco**: I messaggi di smishing sembrano provenire da fonti legittime come banche, enti pubblici o aziende note. Questi messaggi spesso contengono link o numeri di telefono che inducono le vittime a fornire dati sensibili[1].
3. **Obiettivi**: I truffatori mirano a ottenere credenziali di accesso, dati personali, informazioni finanziarie e codici OTP per completare transazioni fraudolente[1].
4. **Segnali di allarme**:
   - Messaggi che richiedono azioni urgenti.
   - Link sospetti o numeri di telefono da chiamare.
   - Richieste di dati personali o finanziari[1].
5. **Come proteggersi**:
   - Non cliccare su link o rispondere a messaggi sospetti.
   - Verificare l'autenticità dei messaggi contattando direttamente l'ente o l'azienda.
   - Attivare notifiche per monitorare le transazioni bancarie[1].
6. **Cosa fare se si è vittima**:
   - Denunciare il reato alla Polizia Postale.
   - Informare la propria banca o l'ente coinvolto.
   - Richiedere il risarcimento dei danni subiti, se possibile1.

PHISHING DI RECONNAISSANCE



- Serve per capire se esiste un account
- Il phishing di reconnaissance è una tecnica di cyber-crimine in cui i criminali informatici raccolgono informazioni sulle potenziali vittime per creare messaggi di phishing mirati.
- Il phishing di reconnaissance può includere la scansione di siti web, l'analisi di social media e l'utilizzo di strumenti di raccolta di informazioni online.
- Il phishing di reconnaissance può aiutare i criminali informatici a creare messaggi di phishing credibili che sembrano provenire da fonti legittime.

COS'È UN EMAIL SPAM CREDENTIAL HARVESTER?



- Un email spam Credential Harvester è una forma di phishing in cui viene creata una pagina web fraudolenta per l'acquisizione di informazioni personali e di accesso
- Questa tecnica di phishing è in grado di catturare informazioni come nomi utente, password e informazioni di conto bancario
- I criminali informatici utilizzano questi dati rubati per commettere frodi finanziarie o rubare l'identità
- Il modo migliore per proteggersi dagli attacchi di phishing è di essere vigili e di non fornire informazioni personali o di accesso a siti web sconosciuti.

COS'È UN'EMAIL SPAM SOCIAL ENGINEERING (RAPPORT FASULLI)?

- L'email spam Social Engineering è una tecnica di phishing in cui gli hacker utilizzano l'ingegneria sociale per convincere le vittime a rivelare informazioni personali o finanziarie.
- Il Social Engineering utilizza spesso false promesse o minacce per indurre le vittime a fornire informazioni riservate.
- I criminali informatici possono utilizzare l'email spam Social Engineering per rubare informazioni di accesso, informazioni di conto bancario o per installare software dannoso sui computer delle vittime.

COS'È L'EMAIL SPAM WHALING

- Lo spam Whaling è una forma di phishing mirata a dirigenti o funzionari di alto livello.
- Il Whaling mira a rubare informazioni riservate come password, informazioni bancarie e dati aziendali.
- Il Whaling utilizza tecniche di ingegneria sociale per convincere le vittime a fornire informazioni riservate.
- Le email Whaling spesso sembrano provenire da fonti legittime e possono contenere allegati o link dannosi.

COS'È UN'EMAIL SPAM MALICIOUS FILES?

- L'email spam Malicious Files è una forma di phishing che utilizza file dannosi per rubare informazioni personali.
- Gli spam di Malicious Files spesso contengono allegati o link che distribuiscono malware sui computer delle vittime.
- L'email spam Malicious Files può causare la perdita di dati, danni al computer e altri problemi di sicurezza.

Tipi di Attacco Phishing

- **SPEAR PHISHING** – L'attaccante investe tempo e SE per creare un rapporto con la vittima
- **IMPERSONATION** – L'attaccante si finge chi non è
- **TYPOSQATTING ED OMOGRAFIA** – L'uso di domini simili con differenti lettere o caratteri di altri linguaggi che simulano i domini reali.
- **SENDER SPOOFING** – preceduto dall'harvester è una vera mail «rubata»
- **HTML STYLING** – E' la ricostruzione di form reali di mail ricevute
- **ATTACHMENTS** – Comprendono file nocivi e non nocivi fasulli
- **HYPERLINKS** – Sono presenti link malevoli nelle mail
- **URL SHORTENING** – E' la possibilità di accorciare i link per renderli appetibili
- **USE LEGITIMATE SERVICES** – Vengono usati servizi validi (outlook.com) per email fasulle
- **BUSINESS EMAIL COMPROMISE** – è la compromissione di un vero indirizzo aziendale

COSA È LO SPEAR PHISHING?

- Lo SPEAR PHISHING è una forma di phishing altamente mirata in cui i criminali informatici investono tempo e sforzi per creare un attacco personalizzato contro una singola persona o un gruppo ristretto.
- Gli attaccanti cercano di raccogliere informazioni specifiche sulla vittima o sul gruppo per creare un attacco efficace.
- Lo SPEAR PHISHING può includere l'invio di e-mail o messaggi di testo fraudolenti, con l'obiettivo di indurre la vittima a fare clic su link o scaricare allegati dannosi.
- Le misure di sicurezza come l'educazione degli utenti, la verifica dell'indirizzo email del mittente e l'utilizzo di software antivirus aggiornati possono aiutare a prevenire gli attacchi di SPEAR PHISHING.

COS'È L'IMPERSONATION PHISHING?

L'impersonation phishing :

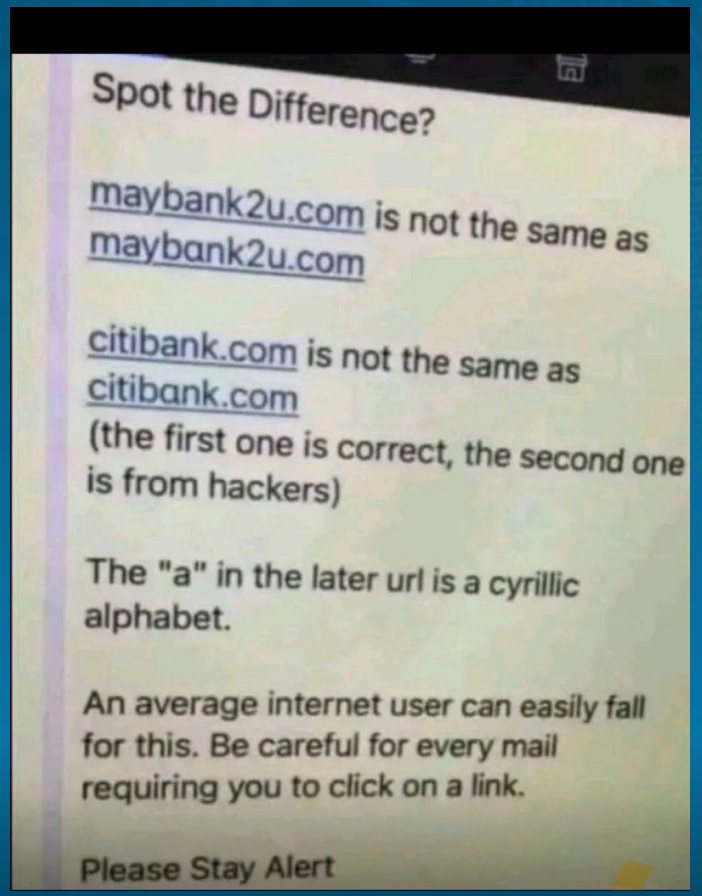
- è una forma di phishing in cui i truffatori si fingono una persona o un'organizzazione che la vittima conosce e in cui confida per ottenere informazioni personali.
- può avvenire tramite e-mail, messaggi di testo, messaggi diretti sui social media o tramite chiamate telefoniche.
- può portare alla divulgazione di informazioni personali sensibili come password, numeri di carta di credito o dati di accesso.

Alcune tecniche utilizzate nell'impostazione phishing includono l'utilizzo di indirizzi e-mail fasulli, l'imitazione di siti web legittimi e l'utilizzo di messaggi che inducono le vittime a cliccare su link o scaricare allegati dannosi.

COS'È IL TYPOSQUATTING E L'OMOGRAFIA

- Il typosquatting è una tecnica di phishing in cui i truffatori registrano domini Internet con nomi simili a quelli di aziende o siti web legittimi.
- L'omografia è una tecnica di phishing in cui i truffatori utilizzano caratteri simili o uguali in nome di dominio o URL per ingannare le vittime.
- Il typosquatting e l'omografia possono essere utilizzati per indurre le vittime a fornire informazioni personali o finanziarie o per installare malware sui loro dispositivi.

TYPOSQUATTING



Il typosquatting è una forma di crimine informatico in cui gli hacker registrano domini con nomi di siti Web noti deliberatamente scritti in modo errato.

Gli hacker lo fanno per attirare ignari visitatori verso siti Web alternativi, in genere per scopi dannosi.

I visitatori possono raggiungere questi siti Web alternativi in due modi:

- Digitando inavvertitamente il nome di siti Web popolari nel browser Web, ad esempio goooogle.com anziché google.com.
- Cadendo vittima di un attacco di phishing più ampio.

COS'È IL SENDER SPOOFING?

- Il Sender Spoofing è una tecnica di phishing in cui l'attaccante falsifica l'indirizzo email del mittente.
- Il Sender Spoofing viene utilizzato per inviare email fraudolente che sembrano provenire da fonti affidabili.
- Il Sender Spoofing può essere utilizzato per indurre le vittime a fornire informazioni personali o finanziarie.

COS'È IL PHISHING HTML STYLING?

- Il phishing HTML STYLING e' la ricostruzione di form reali in email ricevute
- Il phishing HTML STYLING è una tecnica di phishing in cui i truffatori utilizzano il codice HTML per mascherare il vero URL di un link.
- L'URL falso può essere nascosto all'interno della pagina HTML, rendendolo difficile da individuare per l'utente.
- Il phishing HTML STYLING può anche essere utilizzato per mascherare l'aspetto di un sito web o di una pagina di login, per ottenere le credenziali degli utenti.

IL PHISHING ATTACHMENTS

- Il phishing attachments è una tecnica di phishing in cui i truffatori utilizzano allegati di posta elettronica per ingannare le vittime e rubare informazioni personali.
- Gli allegati di posta elettronica possono essere documenti, immagini, file audio o video che sembrano innocui.
- L'apertura di un allegato di phishing può causare il download di malware sul computer o fornire ai truffatori l'accesso alle informazioni personali dell'utente.

PHISHING HYPERLINKS

- Il phishing Hyperlinks è una forma di phishing in cui i truffatori inseriscono un link dannoso all'interno di un'e-mail o di un messaggio di testo, con l'obiettivo di rubare informazioni personali o finanziarie.
- Gli hyperlink di phishing spesso sembrano provenire da fonti affidabili, come le banche o le società di carte di credito.
- Gli utenti dovrebbero evitare di fare clic su link sospetti o di fornire informazioni personali a siti web non affidabili.
- Le tecniche di prevenzione includono la verifica dell'URL di destinazione e l'installazione di software antivirus affidabile.

COS'È IL PHISHING URL SHORTENING

- Il phishing URL shortening è una tecnica di phishing in cui i truffatori utilizzano URL accorciati per nascondere l'indirizzo di un sito web.
- Il phishing URL shortening viene utilizzato per ingannare le vittime a fare clic su link dannosi.
- I truffatori utilizzano spesso servizi di accorciamento URL come bit.ly o goo.gl per mascherare l'indirizzo del sito web.
- Gli utenti dovrebbero evitare di fare clic su link sospetti o di fornire informazioni personali a siti web non affidabili.

PHISHING USE LEGITIMATE SERVICES

- Il phishing Use Legitimate Services utilizza servizi legittimi per inviare e-mail fraudolente.
- Gli attaccanti utilizzano servizi come Outlook o Gmail per creare e-mail che sembrano provenire da fonti affidabili.
- Il phishing Use Legitimate Services può essere difficile da individuare poiché le e-mail sembrano provenire da fonti affidabili.

COS'È IL PHISHING BUSINESS EMAIL COMPROMISE?

- Il Business Email Compromise (BEC) è una forma di phishing mirata a organizzazioni e imprese.
- Il BEC si verifica quando gli hacker si fanno passare per un'organizzazione di fiducia e inviano e-mail fraudolente per rubare informazioni o denaro.
- Il BEC è spesso utilizzato per rubare informazioni di accesso a conti bancari, informazioni finanziarie e dati di identificazione personale.
- Il modo migliore per proteggersi dal BEC è di essere vigili e di educare gli utenti a riconoscere le e-mail fraudolente.

Artefatti del Phishing

In una mail di phishing, ci sono alcuni dati, chiamati «artefatti» che servono per fare una corretta inspection della mail e capirne la provenienza.

Si dividono in tre categorie:

- Artefatti della email
- Artefatti dei file
- Artefatti del web

EMAIL ARTIFACTS

- Sending Email Address: indirizzo del mittente
- Subject Line: l'oggetto della mail
- Recipient Email Address: il destinatario della mail
- Sending Server IP e Reverse DNS: l'IP di partenza ed il DNS Name
- Reply-to Address: in caso sia presente l'indirizzo di risposta
- Date & Time: il timestamp dell'invio del messaggio

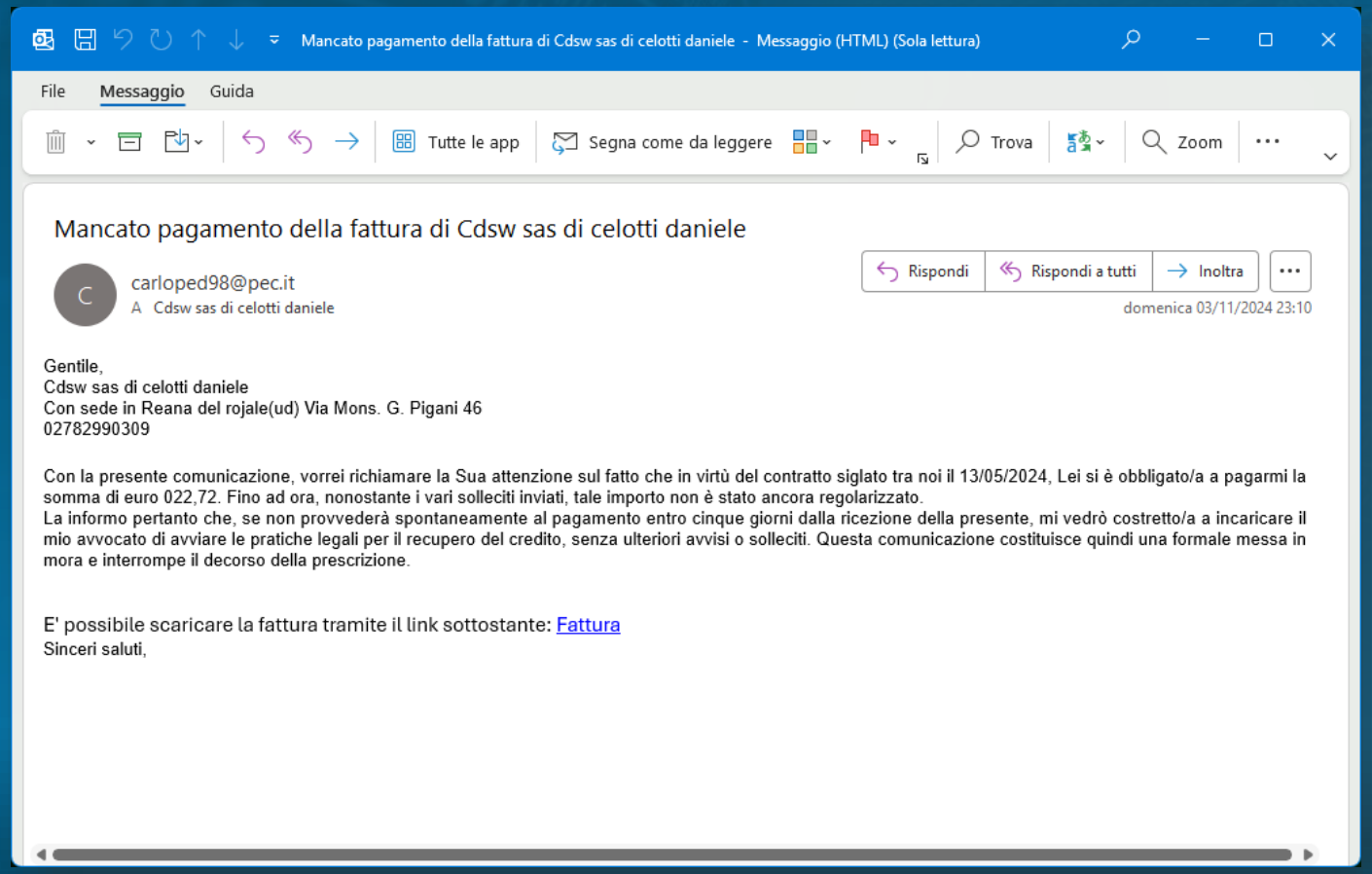
FILE ARTIFACTS

- Attachment Name: il nome del file o dei file
- SHA256 Hash Value: l'hash del file

WEB ARTIFACTS

- FULL URLs: i link completi dei puntamenti
- Root Domain: il root domain degli url allegati (non è essenziale)

PHISHING EMAIL AND/OR PEC (?) MESSAGE



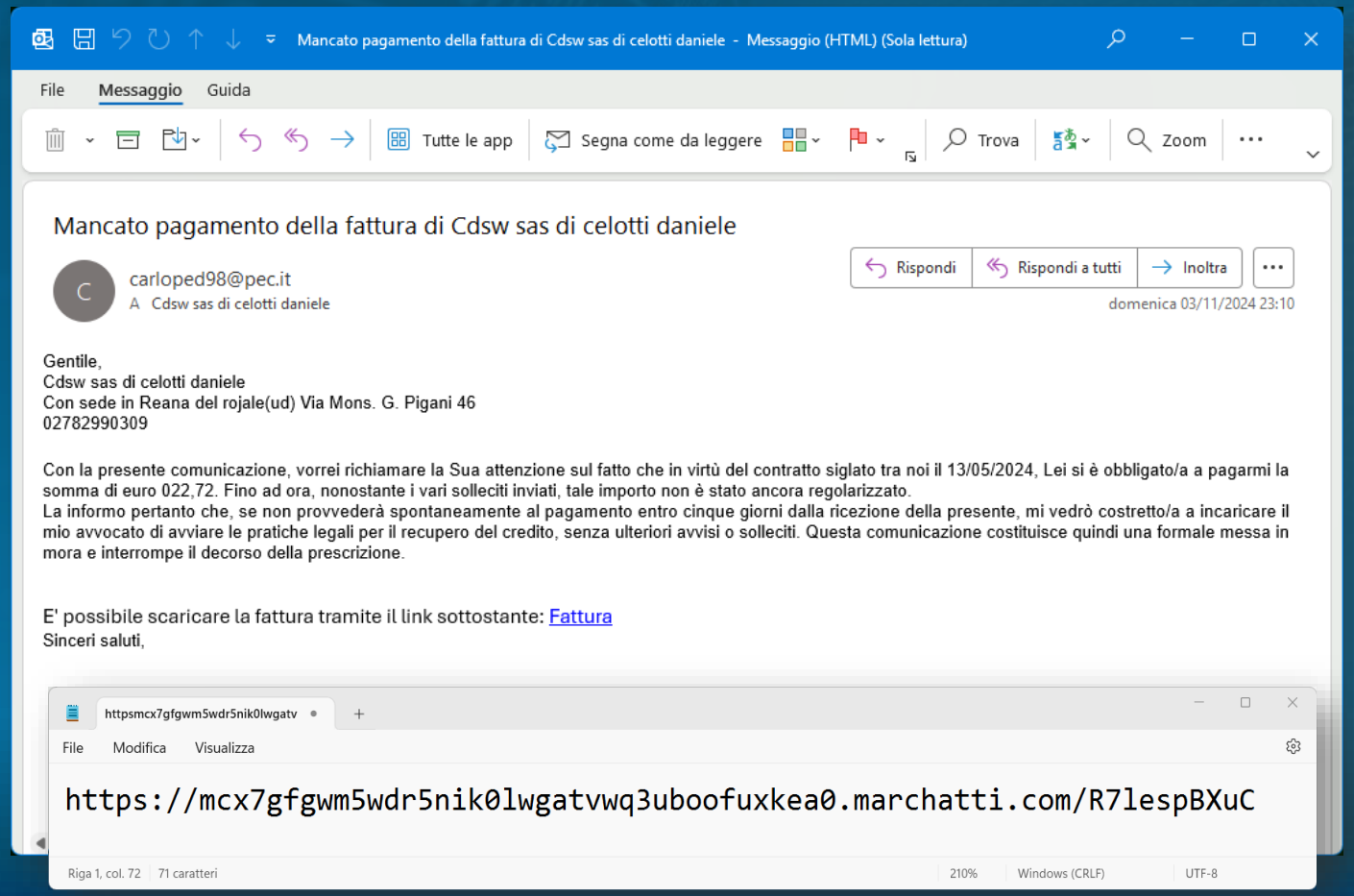
Analisi errori:

- Gentile, nome a capo dopo la virgola
- Nome azienda (maiuscole-minuscole)
- Nome località
- In data 13 maggio non c'è stato nulla ➔ calendario
- Importo basso (022,72) ➔ non conviene avvocato
- Nessun sollecito
- Regolarizzare un importo ➔ poco usato
- Sinceri saluti e non si firma

Ricerca storico

- Come riconoscere una PEC falsa ed evitare le truffe

PHISHING EMAIL AND/OR PEC (?) MESSAGE



Email existence checker:
- Verifying the Email - Email Checker
- Free email address validator
- Free Email Address Verifier emailhippo.com

Link checker:
- Site-Shot - Capture a Website screenshot
- Screenshotmachine.com/
- VirusTotal – Home
- Browserling - Live interactive
- Screenshot.guru

Analisi del Dominio:
- Whois marchatti.com
- www.geolocation.com (via IP address)
- Whois Lookup ➔ indirizzo ➔ Maps

COS'È UN'EMAIL SPAM FALSO POSITIVO?

- Un'email spam falso positivo si verifica quando un programma antivirus identifica un'email legittima come spam.
- Ciò può accadere a causa di filtri antispam troppo rigorosi o configurazioni antivirus errate.
- Un'email spam falso positivo può portare alla perdita di messaggi importanti o alla diminuzione della produttività.

Come evitare il phishing

- **Descrizione: Truffa via email che mira a rubare informazioni personali.**
- **Come Riconoscerlo:**
- Email da mittenti sconosciuti o sospetti.
- Richieste urgenti di informazioni personali.
- Link sospetti o allegati pericolosi.
- **Consigli:**
- Non cliccare su link sospetti.
- Verificare sempre l'indirizzo del mittente.
- Utilizzare software antivirus aggiornati.

CONCLUSIONI

- Lo spam phishing è una tecnica di truffa online per rubare informazioni personali.
- Esistono diversi tipi di spam phishing, tra cui il phishing di reconnaissance, il phishing di spam e il phishing di ingegneria sociale.
- È importante essere vigili e utilizzare misure di sicurezza come la verifica dell'URL di destinazione e l'installazione di software antivirus affidabile.