

# FURTI DI IDENTITA' E TRUFFE INFORMATICHE



**ADICONSUM**

Associazione Difesa Consumatori APS

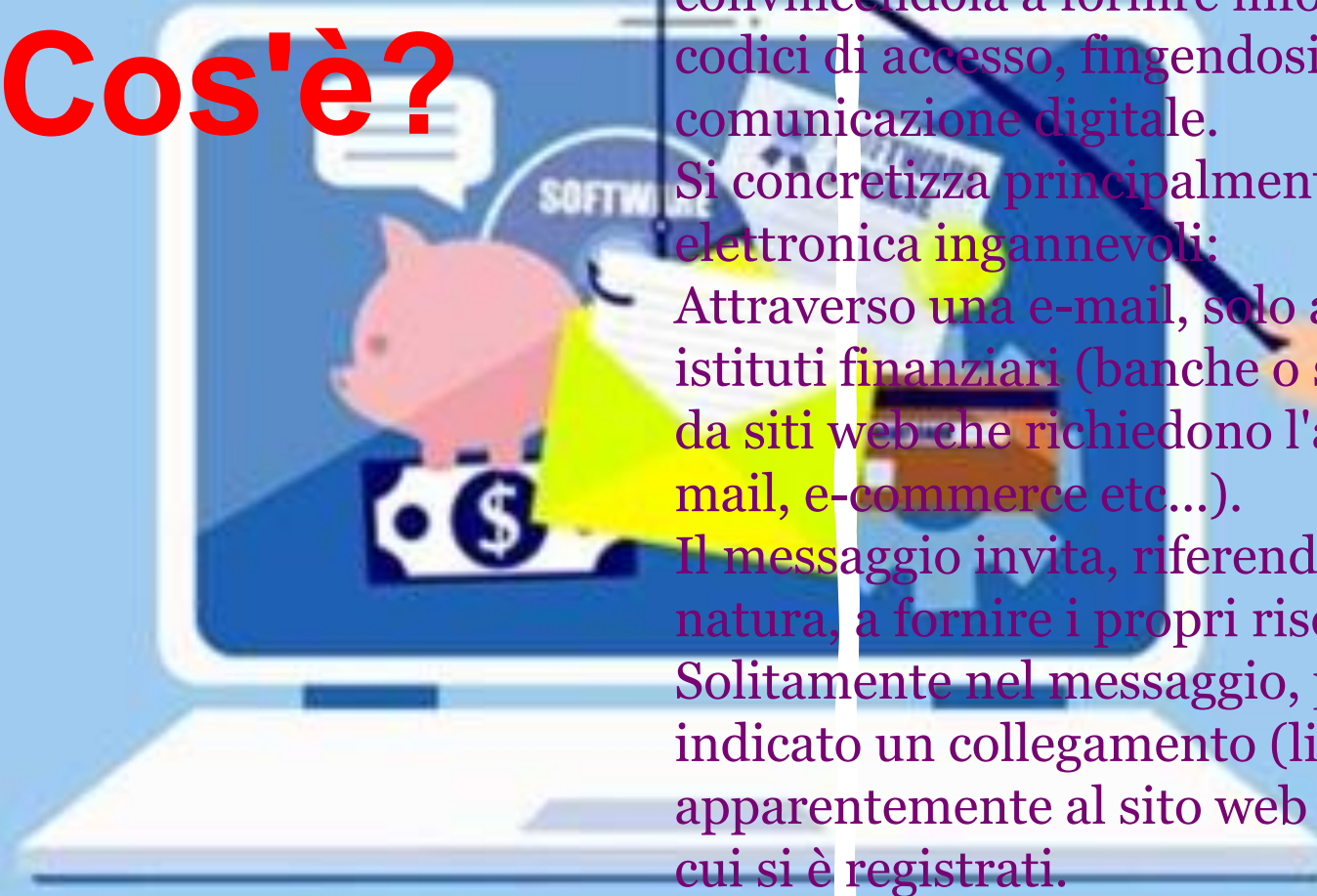
*dal 1987*



# II Phishing

Sara Denisa Irimia, Gaia Hadoui, Alessandra Raschellà, Salma Malyana

# Che Cos'è?



Il Phishing è un tipo di truffa effettuata su internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli:

Attraverso una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce etc...).

Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio. Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati.



Esistono varie tipologie di Phishing,  
ma le più diffuse sono:



# Random Phishing

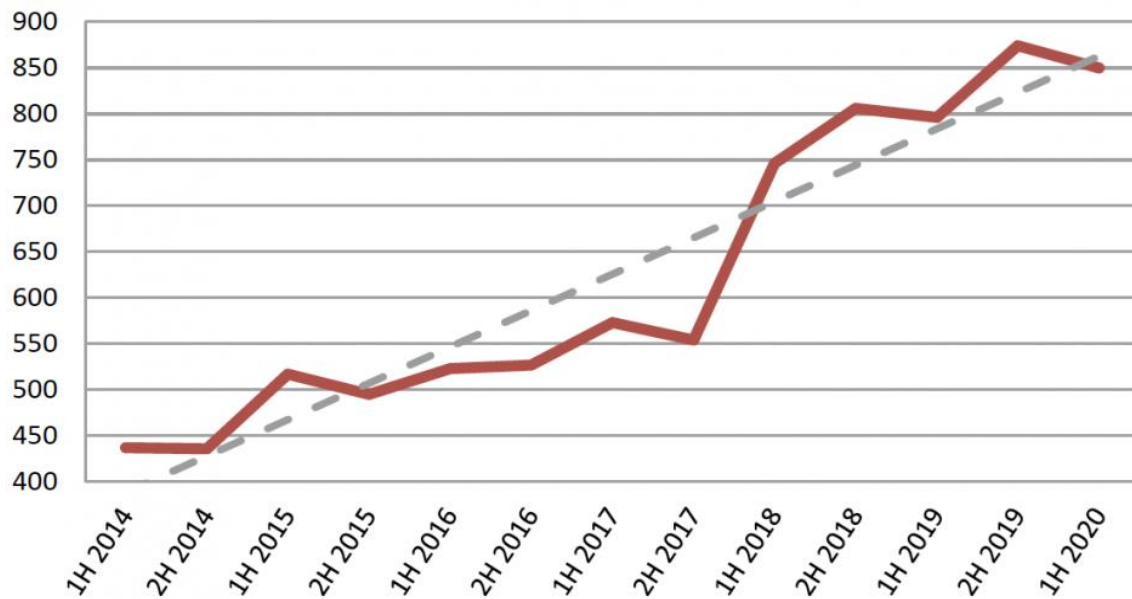
---



Il Random Phishing consiste nell'invio massivo di e-mail. In altre parole, un hacker si dota di un indirizzo e-mail che a prima vista può sembrare attendibile e diffonde messaggi in riferimento a problemi tecnici, procedure di aggiornamento software o tentativi di accessi indesiderati. Il messaggio invita l'utente a cliccare su un link.

# Clone Phishing

Numero di attacchi gravi per semestre (2014 1H 2020)



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia - aggiornamento giugno 2020

In questo tipo di Phishing, l'autore della truffa clona un' e-mail autentica che potresti aver ricevuto da un mittente "reale" ma inviata da un ID e-mail falsificato. Il truffatore crea una e-mail autentica che intercetta o che può far parte di un messaggio precedente che il destinatario ha inviato al mittente. Questa copia di posta elettronica contiene contenuti dannosi come un collegamento, che cliccato, porta all'istallazione di malware sul tuo sistema.

# Vishing

---

Quando si dice che il Phishing si può non solo vedere ma anche sentire, questo è il caso. Squilla il vostro telefono. Alzate la cornetta e dall'altro lato vi risponde una voce autorevole e professionale:

**"Buonasera signora \*\*\*\*, sono di Unicredit Banca, abbiamo rilevato un ingresso sospetto al suo portale dell'home banking. Gentilmente se volesse fornirmi i suoi dati facciamo una verifica interna e le riabilitiamo tutte le funzioni del conto".**

Detta così non fa una piega. Peccato che la telefonata arrivi da un centralino VoIP non di proprietà di Unicredit. In questo caso la centralinista rientra tra gli elementi dell'attacco Vishing.

Dunque, il Vishing, è una forma di truffa simile al Phishing; con lo scopo di carpire con l'inganno informazioni private, e viene effettuata tramite servizi di telefonia.

# Social network Phishing



**SOCIAL NETWORK  
UN PERICOLO PER I  
GIOVANI SE USATO  
SENZA CONTROLLO**

**CYBER RISK**

Un attacco di Phishing sui social media è dove l'hacker utilizza i nostri siti di social media preferiti, da Facebook a Instagram, per rubare i nostri dati personali; di solito inserendo nelle pagine dei nostri amici o colleghi qualcosa su cui non possiamo resistere di cliccare.

Le informazioni raccolte dagli hacker includono credenziali di accesso all'account di social media, informazioni sulla carta di credito e fatti personali su una determinata persona che potrebbero quindi essere utilizzati per lanciare altre truffe e tipi di attacchi fraudolenti.



**"Ci hanno telefonato con il numero della banca: via 48mila euro"**



# Come proteggersi dal phishing

---

Consigli per la tua  
sicurezza digitale



# Anti-phishing

---

L'anti-Phishing è la strategia per la difesa da mail sospette e dal Phishing; è ormai diventato un'importante necessità.

Tutti noi riceviamo quasi quotidianamente mail autentiche che sembrano provenire da istituti di credito, istituzioni pubbliche, amici, colleghi di lavoro etc... In queste e-mail sono spesso contenuti allegati di vario genere o link che in apparenza sembrano veritieri; spesso quindi l'anti-virus non segnala minacce.

Il software anti-phishing è costituito da programmi per computer che tentano di identificare il contenuto di phishing in siti web, e-mail o altri moduli utilizzati per accedere ai dati e bloccarne il contenuto, generalmente con un avviso all'utente.



**ANTI-PHISHING**  
IL MEGLIO DELLA SICUREZZA INFORMATICA

# Come proteggersi dal phishing

---

Consigli per la tua  
sicurezza digitale

- Se arriva una e-mail dove chiede di modificare informazioni personali è meglio non fidarsi.
- Controlla l'URL del link.
- Non compilare mai campi all'interno della mail.
- Non aprire gli allegati della mail che non hai richiesto o che non conosci.
- Non rivelare a nessuno le tue password e cambiale spesso.
- Usa un anti-virus e un software anti-fishing

[www.giovanrifalcone.it](http://www.giovanrifalcone.it)

SOS

Segnalazioni di Operazioni Sospette

# Come riparare al danno subito?

---

Se si cade vittima di un attacco di phishing, la prima cosa da fare è bloccare immediatamente l'account vittima dell'attacco.

Cambiare la password, contattare il servizio clienti.

Qualora l'account sia già stato compromesso e non si è più possibile fare il login con i propri dati, è necessario contattare il servizio clienti per ripristinare manualmente i vostri dati d'accesso.

Nel caso di furto di dati bancari, invece, va contattato l'istituto di credito per bloccare i servizi coinvolti dalla truffa (carte di credito, conti correnti, bancomat,...). Avvisare gli enti colpiti. Oltre per dei dati personali, è segnalare l'attacco Phishing agli enti che ne sono stati colpiti, così che possono prendere provvedimenti e contrastare la truffa.

Il passo successivo invece, è informare le autorità competenti.

# A chi denunciarlo?

---

**Il Phishing, se pur possa sembrare una semplice e-mail ingannevole è un reato vero e proprio e come tale va considerato. In quanto reato informatico inoltre, va comunicato alla Polizia Postale, che sul suo sito ha disposto uno spazio per le segnalazioni di questo tipo.**

**La stessa Polizia Postale, sul suo portale, raccoglie gli avvisi ricevuti classificati come Phishing. Consultando quella pagina è possibile farsi un'idea sui tentativi di frode in corso, ed eventualmente avere la conferma che le e-mail ricevute fanno parte di quella categoria.**

## **ATTENZIONE:**

**Se si riceve una mail che rimanda a un sito di Phishing è importante non selezionare il link ma segnalare la comunicazione alla Polizia**

# Denunciare il furto di identità

---

**Il furto di identità è un reato  
sia che si tratti di sostituzione di persona  
che di frode informatica.  
Pertanto dovrà sempre essere denunciato  
alle Forze dell'Ordine**

Ma è anche consigliabile segnalare il fatto  
all'Autorità Garante per la protezione dei dati personali ([www.garanteprivacy.it](http://www.garanteprivacy.it))  
e alla Autorità delle Telecomunicazioni ([www.agcom.it](http://www.agcom.it))

# Frode sul c/c o sulla carta di credito





# In caso di attivazione pratiche di finanziamento





# Denuncia penale

---

Dopo il disconoscimento dell'operazione nei confronti della Banca, occorre sempre procedere con **querela**, atto che dovrà poi essere messo a disposizione della Banca o della Posta.

# Furto sui Social Network

---

IL FATTO DOVRA' ESSERE IMMEDIATAMENTE SEGNALATO  
ALLA PIATTAFORMA

fare copia autentica del profilo online creato coi nostri dati

Facebook

<https://it-it.facebook.com/help/>

Google

<https://www.google.it/intl/it/con>

Twitter

<https://help.twitter.com/it>



---

*Ricordiamo infine che le Associazioni dei Consumatori sono a disposizione delle vittime di furto di identità per aiutare nel redigere le denunce, ricorsi all'ABF e valutare l'opportunità di agire in giudizio per ottenere il risarcimento di tutti i danni subiti dall'utente.*