Le Frodi Informatiche

Riconoscerle per difendersi

Relatore Francesco Nassisi
Studio Nassisi | Servizi Informatici
28/11/2017

Sommario

- Cos'è internet e come funziona
- Opportunità e rischi della Rete
- Le frodi informatiche
- Gli autori
- Le motivazioni
- I tipi di frode più diffusi
- Le tecniche di ingegneria sociale
- Come riconoscere un tentativo di frode
- Cattive abitudini e comportamenti a rischio
- Come difendersi: alcuni consigli utili
- Cosa fare se riteniamo di essere vittima di una frode

Relatore Francesco Nassisi
Studio Nassisi – Servizi Informatici

Che cos'è Internet

La «rete delle reti»

Internet: cenni storici

- Anni ‘50: inizia a farsi strada l’idea di una rete informatica condivisa
- Anni ’80: inizia a diffondersi la tecnologia che è alla base del funzionamento di Internet
- 1986: prima connessione dall’Italia
- Anni ‘90: crescita esponenziale del Web
- 2015: 3,3 mld di dispositivi connessi

Internet: come funziona

- I contenuti della Rete sono organizzati in siti web (insieme di pagine web)
- Ogni pagina web può contenere testi, immagini e contenuti multimediali
- Si può passare da una pagina all'altra grazie a menù, pulsanti e link
- La navigazione è libera, senza alcun ordine predefinito

Internet: le applicazioni

- Comunicazioni (email e cellulari)
- Intrattenimento (film e musica in streaming)
- Trasporti e logistica
- Acquisti (pagamenti elettronici)
- Medicina
- Servizi informativi

L’altra faccia della medaglia

Senza dubbio Internet ha contribuito a modificare l’intera economia mondiale, ma…

non è tutto oro quello che luccica!

Cosa sono le frodi informatiche

Truffe perpetrate da un criminale informatico, attraverso l'intrusione o l'alterazione di un sistema informatico.

L'attacco può interessare anche solo i programmi o le informazioni elaborate dal sistema preso di mira.

Gli autori: hacker

L'hacker è uno specialista di sistemi informatici, conosce le più avanzate tecniche di sicurezza informatica ed è in grado di aggirarle

Le motivazioni

- Economiche
- Politiche
- Religiose
- Etiche
- Vendetta personale

Frodi informatiche più diffuse

Phishing

Furto d’identità

Cos’è il phishing?

E’ un tipo di frode ideato allo scopo di rubare informazioni sensibili e riservate come numeri di carte di credito, password, credenziali di accesso ad account personali della vittima

Le modalità di attacco

- Email
- Siti web progettati ad hoc
- Banner pubblicitari
- Messaggi Whatsapp
- Facebook (fake news)

Phishing: alcuni esempi

INTESA SANPAOLO

Gentile Cliente,

Nell'ambito di un progetto di verifica dei data anagrafici forniti durante la sottoscrizione dei servizi di Intesa Sanpaolo S.p.A. e stata riscontrata una incongruenza relativa ai dati anagrafici in oggetto da Lei forniti all momento della sottoscrizione contrattuale.

L'inserimento dei dati alterati puo costituire motivo di interruzione del servizio secondo gli art. 135 e 137/c da Lei accettati al momento della sottoscrizione, oltre a costituire reato penalmente perseguibile secondo il C.P.P art.415 del 2001 relativo alla legge contro il riciclaggio e la trasparenza dei dati forniti in autocertificazione.

Per ovviare al problema e' necessaria la verifica e l'aggiornamento dei dati relativi all'anagrafica dell'Intestatario del servizio.
Effettuare l'aggiornamento dei dati cliccando sul seguente link:

http://www.intesasanpaolo.com/scriptlbve/retail20/o/ita/home/ita_home.jsp

Cordiali Saluti

Oggetto: La password de la sua carta Flash! **Ricevuto il:** 09/08/09 15:43

INTESA SANPAOLO

La password de la sua carta Flash e stata inserita piu di tre volte.
Per proteggere la sua carta abbiamo sospenso il acceso.

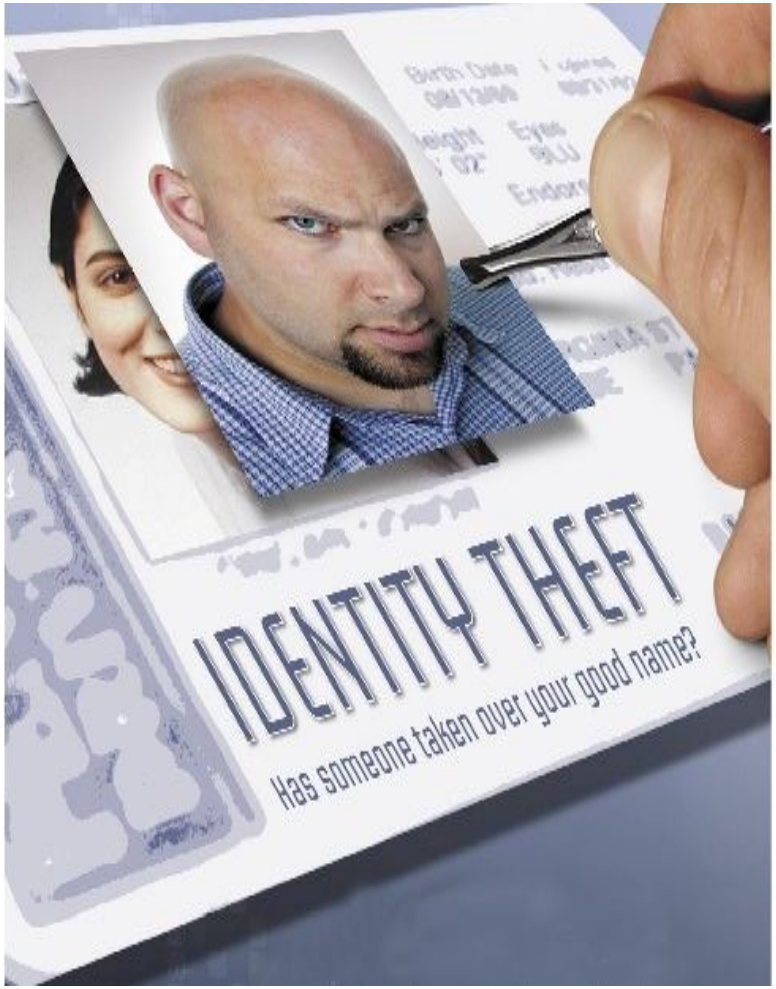
Per recuperare il acceso clicca su :

https://www.monetaonline.it/layout/03069/pop/code-identificazione-31357819513/

Grazie ancora per aver scelto i servizi on-line di carta FLASH.
I migliori saluti.

Servizio Clienti IntesaSanPaolo

Il furto d’identità



Ha per oggetto l'identità di una persona: l’hacker riesce ad assumere l’identità di un utente sfruttando le informazioni personali che riesce a raccogliere sulla vittima.

Il fine ultimo del criminale è quello di spendere il nome altrui per ottenere un profitto o compiere azioni illegali a nome della vittima.

Il furto d'identità

- È il tipo di frode più pericolosa;
- La possibilità di subire un furto d'identità non dipende solo dalla nostra imprudenza;
- Oltre al danno economico può avere ripercussioni emotive molto gravi;
- L'hacker può utilizzare l'identità rubata anche per commettere illeciti

Il «modus operandi» dell'hacker

Il criminale informatico riesce a carpire informazioni personali riservate della vittima attraverso sofisticate tecniche di

INGEGNERIA SOCIALE

Le leve dell'ing. sociale

- Autorevolezza
- Senso di colpa / imbarazzo
- Panico
- Desiderio
- Avidità / possesso
- Compassione / buoni sentimenti

Esempi di phishing

- False cartelle esattoriali
- False fatture commerciali
- False bollette telefoniche o del servizio elettrico
- Falsi solleciti di pagamento
- False lettere di vettura dei più noti corrieri nazionale (Bartolini, SDA, DHL)
- Ingiunzioni di pagamento di vario tipo

Come riconoscere il phishing

- Mantenere la calma qualunque sia il tenore del messaggio
- Fermarsi a riflettere su alcuni elementi essenziali della email ricevuta

Come riconoscere il phishing

1. Campo «mittente»
2. Formula di apertura
3. Contenuto del messaggio
4. Link
5. Allegati

Falsi miti da sfatare

- L'antivirus installato sul mio sistema mi garantisce sicurezza al 100%
- Navigo sempre e solo su siti sicuri
- Non ho nulla di importante da proteggere sul mio computer

Perché proteggere il proprio PC

Gli hacker sono sempre interessati a qualsiasi informazione personale sia possibile rastrellare in Rete

Consigli utili

- Non dimenticate mai che Internet è un «luogo» pubblico;
- La pubblicazione implica la perdita di controllo sull'informazione;
- Fate attenzione a ciò che pubblicate;
- Eseguite una navigazione attenta e non cedete alla curiosità;
- Scegliete sempre password lunghe e complesse e proteggetele adeguatamente;

Relatore Francesco Nassisi
Studio Nassisi – Servizi Informatici

Come gestire le password

Non lasciamo le nostre password in giro ed evitiamo di annotarle su agende e foglietti

È molto importante

- Non rispondete mai a messaggi che richiedono informazioni personali;
- Utilizzate più caselle email;
- Evitate di far utilizzare il PC ai bambini senza un'adeguata supervisione;
- Non lasciate mai incustodito il vostro dispositivo;
- Se dovete gettare bollette o ricevute, prima distruggetele affinché non possano essere recuperate;

Protocolli di sicurezza

Per riconoscere un sito sicuro fate attenzione a quanto riportato in alto a sinistra nella finestra del browser

Dispositivi mobili

Tablet e smartphone vengono utilizzati da un numero sempre maggiore di persone

Consigli per l'uso

- Prestate attenzione alle app che scaricate;
- Verificate i permessi richiesti prima di accettare le condizioni d'uso;
- Spesso le app richiedono autorizzazioni insidiose e del tutto superflue;
- Non sottovalutare la quantità di informazioni contenute nei vostri dispositivi mobili

I social network

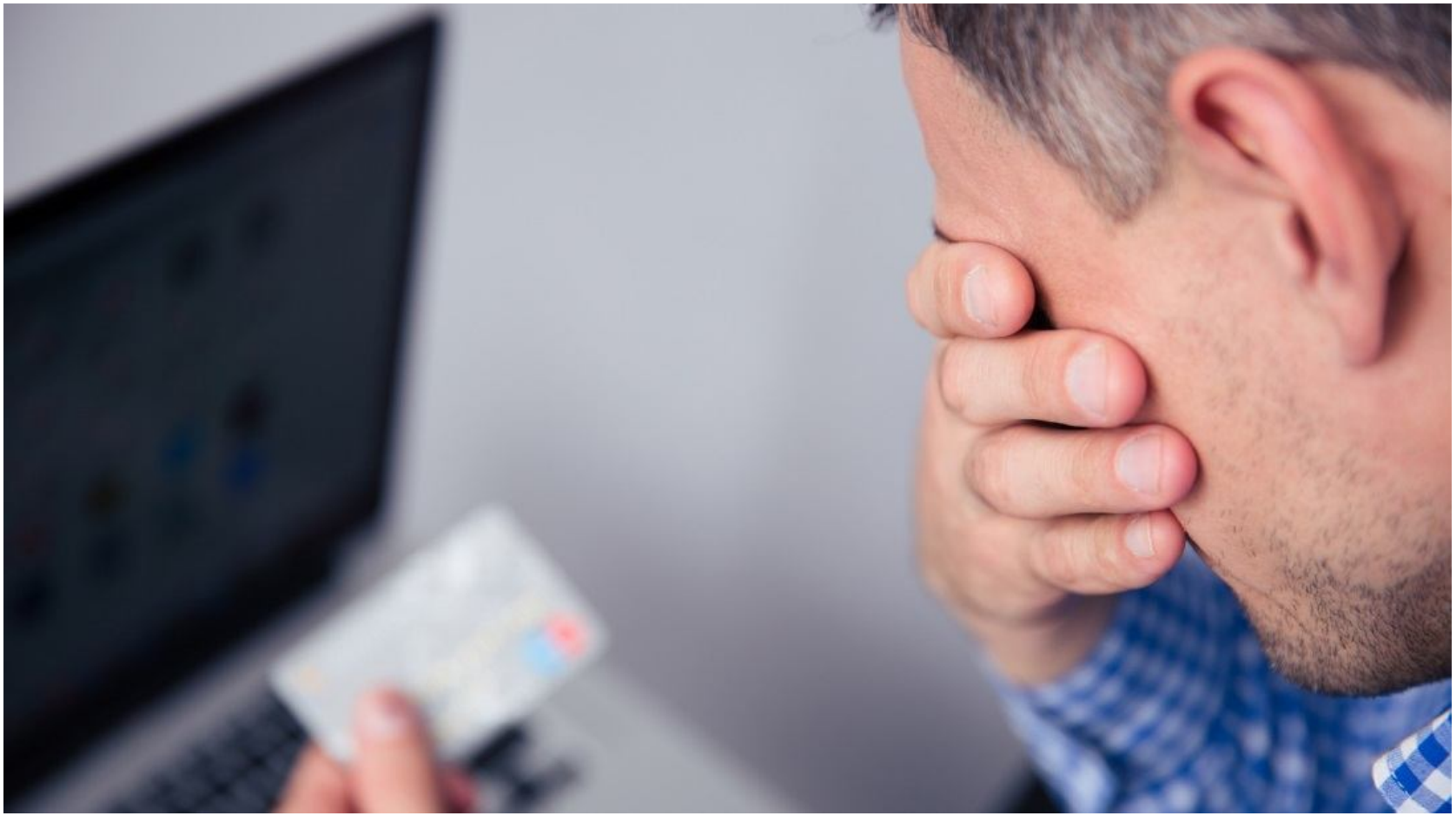
- Rischi nascosti
- Istruzioni per l'uso
- Fake news

Relatore Francesco Nassisi
Studio Nassisi – Servizi Informatici

Connessioni WI-FI aperte

- Come funziona una rete wireless;
- Vulnerabilità di una connessione wi-fi;
- Rischi delle connessioni wi-fi aperte;
- Modalità di intrusione in una rete wi-fi

E se restiamo comunque vittima di una frode informatica?



Cosa fare?

- È essenziale agire immediatamente al fine di limitare i danni;
- Se il problema riguarda degli strumenti finanziari è necessario bloccarli subito;
- Cambiare i codici di accesso al proprio conto;
- Cambiare la password di accesso della casella email collegata al conto o alla cdc;
- Presentare denuncia alla Polizia Postale;
- Se si sospetta anche un furto d'identità può essere utile interpellare un consulente esperto in sicurezza informatica

Grazie a tutti!