Donne Digitali 2019

Sicurezza informatica

Identità digitali

- Ci rappresentano in internet
  - Username, password, informazioni di profilo
- Quante sono?
  - Una per ogni servizio?
  - Una per ogni diverso username?
- Chi le gestisce?
- Hanno un valore economico?

Esempi di data leak

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Verifica

haveibeenpowned.com

Bonus

A chi piacciono le parole crociate?

zed0.co.uk/crossword/

Problemi legati alle password

- Scelta della password
  - Banale (12345678, password, qwerty…)
  - Informazioni personali (nomi di figli, mariti, animali, date di nascita)
  - Difficile, ma con schemi prevedibili (sd53$k+facebook, sd53$k+amazon)
- Gestione delle password
  - Riuso
  - Longevità eccessiva…

Robustezza della password

www.passwordmeter.com

Ok, ma come me le ricordo?

… niente da fare, non si ricordano…

Ma ci sono i password manager!

Esempi notevoli di password manager

https://twitter.com/MikeLDalton/status/95311215731436339 2

https://nakedsecurity.sophos.com/2012/11/21/prince-william-photos-password/

https://www.securelink.com/blog/post-it-passwords/

https://www.youtube.com/watch?v=_u8Rss3W4Wg

Perchè rubare un profilo?

- Dipende dal servizio…
  - Monetizzazione diretta (home banking)
  - Monetizzazione indiretta (stessa identità, password uguali o troppo simili)
  - Vendita di informazioni a spammer
  - Profilazione
  - Social engineering verso
    - noi
    - i nostril contatti
    - l’organizzazione in cui lavoriamo noi o lavorano I nostril contatti

Social engineering

- Carpire informazioni con la psicologia
- Il Social Engineering prevede un insieme di tecniche psicologiche e non informatiche usate per indurre la vittima a:
  - rivelare i dati personali o sensibili
  - oppure ad aprire degli allegati infetti
  - visitare un sito che magari contenga un dialer o qualche altro materiale pericoloso

- Essendo un insieme di tecniche psicologiche, il social engineering non prevede una preparazione informatica ma una conoscenza della potenziale vittima e del suo contesto
  - ... esempio ...

Tecniche – prima fase

- L’attacker ha bisogno di molte informazioni che gli serviranno per essere credibile e convincente con l’interlocutore vittima
- Questa ricerca è mirata alla conoscenza di vari particolari:
  - Identità «fisica» della vittima (famiglia inclusa)
  - Identità digitali della vittima (mail, account social,…)
  - Attività della vittima reperibili online
  - Contatti (amici nei social, mail nella rubrica, …)
  - Interessi della vittima
  - Posto di lavoro, posti di lavoro precedenti
  - …

Tecniche

- La ricerca di queste notizie avviene nei modi più disparati
  - Social network
  - Google
  - Siti pubblici del datore di lavoro
  - Data leak
  - …

https://www.youtube.com/watch?v=F7pYHN9iC9I

Tecniche

- La ricerca di queste notizie avviene nei modi più disparati
  - Social network
  - Google
  - Siti pubblici del datore di lavoro
  - Data leak
  - …
  - … spazzatura inclusa

Uso dell’e-mail

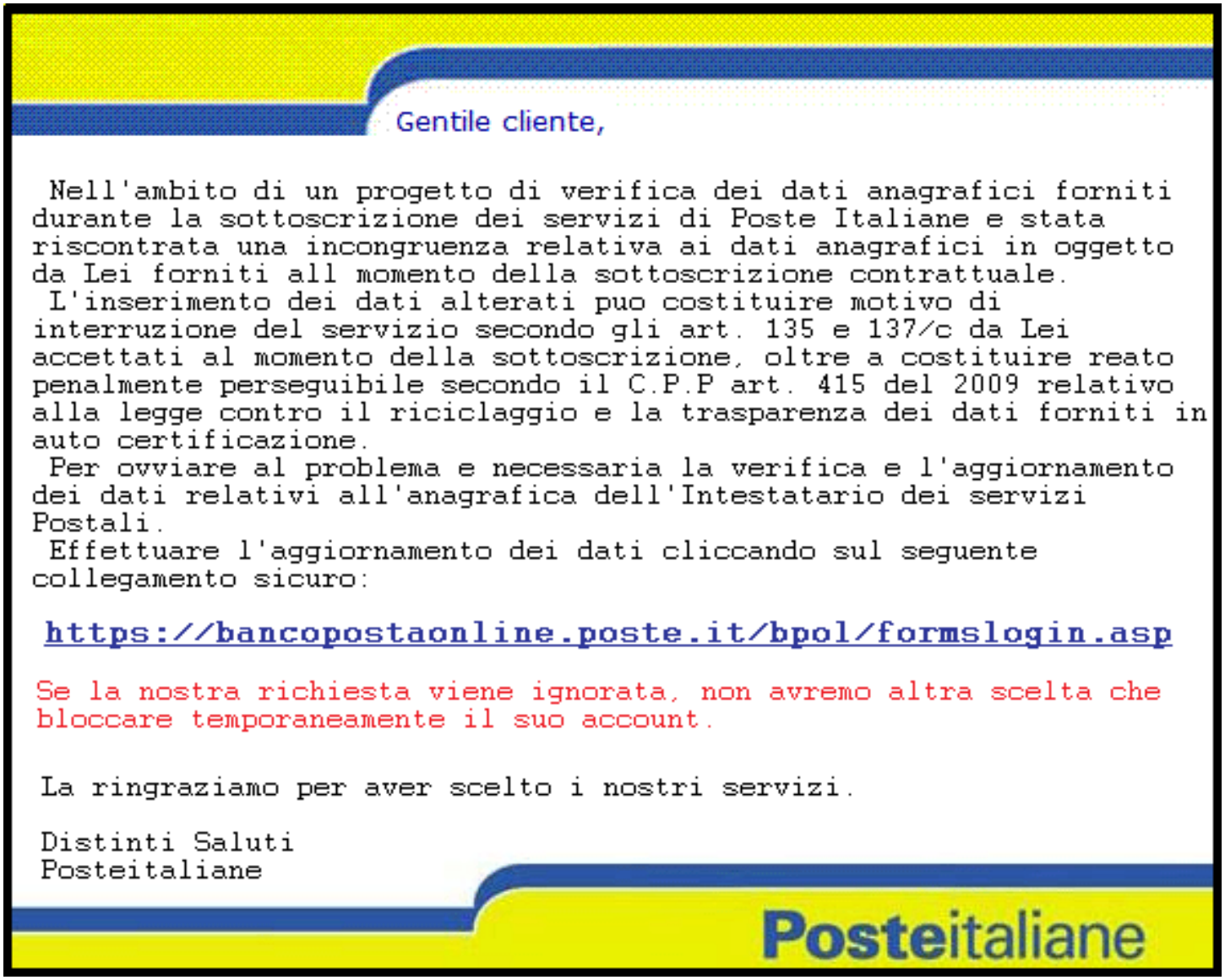
- Se l’attacco avviene via e-mail, bisogna indurre la “vittima”, tramite espedienti psicologici, a fidarsi del contenuto del messaggio e quindi eseguirne i comandi
- Per esempio l’attacker può compilare un messaggio che suggerisce di visitare un falso sito Web, costruito in modo da assomigliare all’originale (es., siti di finanziarie, banche ecc.) per carpire dati sensibili come password, pin, numeri di conto corrente e di carte di credito (phishing)
- Le tecniche di base di questo fenomeno fanno leva su alcune debolezze umane per ottenere i risultati desiderati

Fondamentali

- La social engineering si fonda su alcune caratteristiche della natura umana
  - Desiderio di aiutare
  - Tendenza a fidarsi delle persone che si “accreditano” in qualche modo
  - Paura di incorrere in problemi
  - Senso di colpa

- Un bravo social engineer riesce ad acquisire informazioni senza alimentare alcun sospetto che vuole acquisire informazioni né sulle vere informazioni che intende acquisire
  - Ad esempio, l’attacker fa finta di essere a conoscenza di un’azione illecita perpetuata da parte di qualche collega amico della vittima
  - Quindi finge una complicità e si pone a salvatore presentando una soluzione capace di regolarizzare la posizione dell’utente che ha commesso l’illecito

Esempi di phishing



Gentile cliente,

Nell'ambito di un progetto di verifica dei dati anagrafici forniti durante la sottoscrizione dei servizi di Poste Italiane 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 2009 relativo alla legge contro il riciclaggio e la trasparenza dei dati forniti in auto certificazione.
Per ovviare al problema e necessaria la verifica e l'aggiornamento dei dati relativi all'anagrafica dell'Intestatario dei servizi Postali.
Effettuare l'aggiornamento dei dati cliccando sul seguente collegamento sicuro:

https://bancopostaonline.poste.it/bpol/formslogin.asp

Se la nostra richiesta viene ignorata, non avremo altra scelta che bloccare temporaneamente il suo account.

La ringraziamo per aver scelto i nostri servizi.

Distinti Saluti
Posteitaliane

Posteitaliane

Esempi di phishing

Gentile cliente,

BancoPosta Click

Nell'ambito di un progetto di verifica dei dati anagrafici forniti durante la sottoscrizione dei servizi di Poste Italiane 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 2009 relativo alla legge contro il riciclaggio e la trasparenza dei dati forniti in auto certificazione.

Per ovviare al problema e necessaria la verifica e l'aggiornamento dei dati relativi all'anagrafica dell'Intestatario dei servizi Postali.

Effettuare l'aggiornamento dei dati cliccando sul seguente collegamento sicuro:

https://bancopostaonline.poste.it/bpol/carte/login.asp

Se la nostra richiesta viene ignorata, non avremo altra scelta che bloccare temporaneamente il suo account.

La ringraziamo per aver scelto i nostri servizi.

Posteitaliane

Esempi di phishing

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

Esempi di SMSishing

https://www.money.it/Truffa-SMS-Unieuro-smartphone-in-regalo-attenzione-rischi

Due principali problemi…

- Link
- Allegati

Molte cose sono diverse da come sembrano…

Link

- Non andate sul link contenuto in questa pagina!
  - Potrebbe essere pericoloso…
  - … ma soprattutto rovinate il gioco!

weblab.ing.unimore.it/people/marchetti/link.shtml

Allegati

- Un trucco molto utilizzato: la doppia estensione
  - Fattura.pdf.exe
  - Se l'ultima estensione viene nascosta, può essere che io veda solo Fattura.pdf …

- Utilizzare sempre un antivirus aggiornato!

Virustotal

www.virustotal.com

Altre strategie

Il bravo social engineer è fantasioso…

https://www.youtube.com/watch?v=ZI5fvU5QKwQ

Altre strategie

Vishing

https://www.youtube.com/watch?v=F78UdORll-Q

Internet of Things

- Software e connettività come trend pervasivi…

  - tutto ha username e password …
  - tutti siamo amministratori di sistema…
  - Mai cambiato la password al vostro router / ip cam / stampante / frigorifero connesso / ...

Alcuni problemi

- Credenziali di default mai cambiate…
  - Si trovano facilmente su Internet
  - Tipicamente admin:admin
- Servizi abilitati di default e mai disabilitati, anche se non utilizzati…
  - Esempio: share SMB nelle NAS QNAP