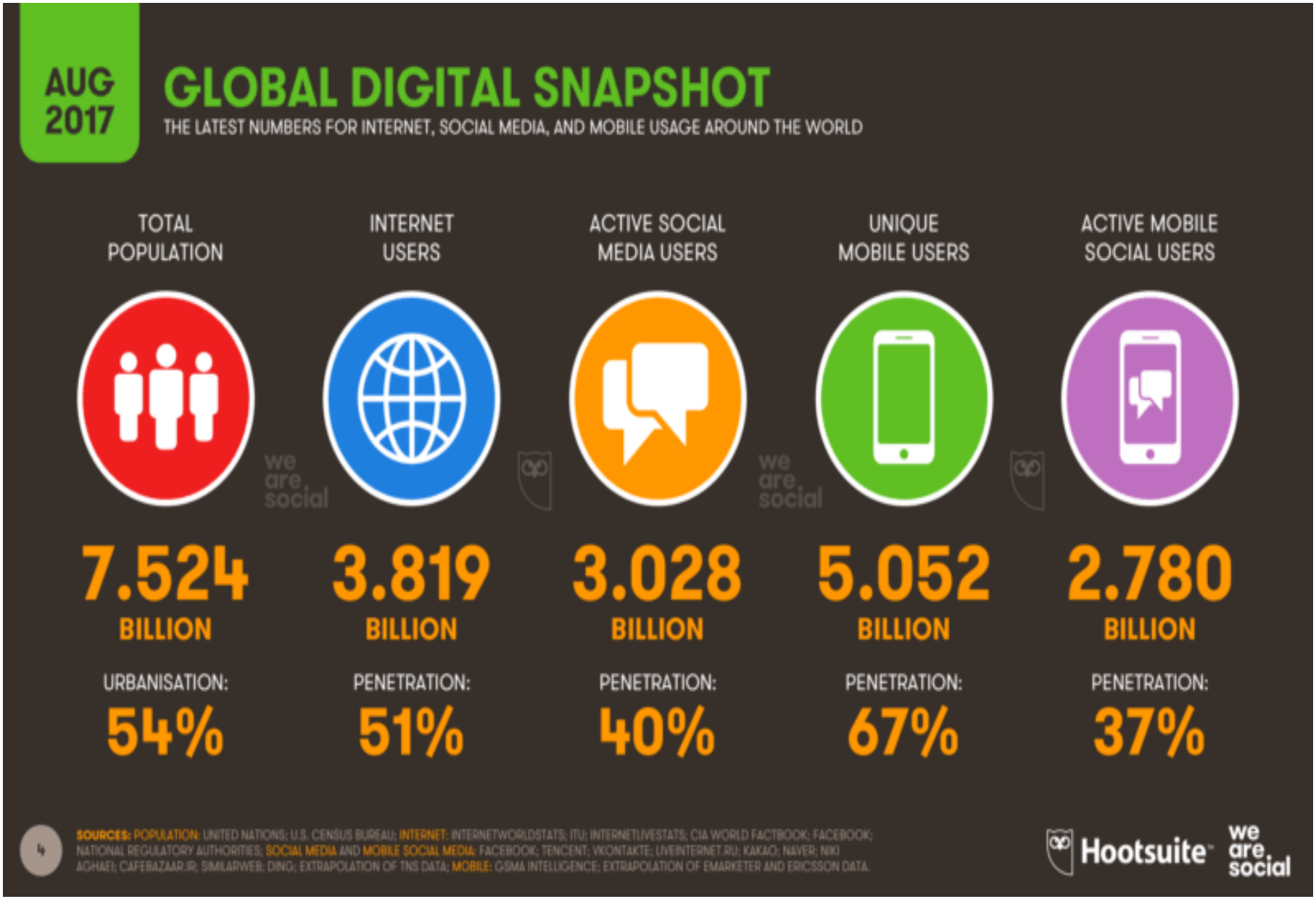
SICUREZZA DELLA RETE INTERNET

Giovanni Parascandolo

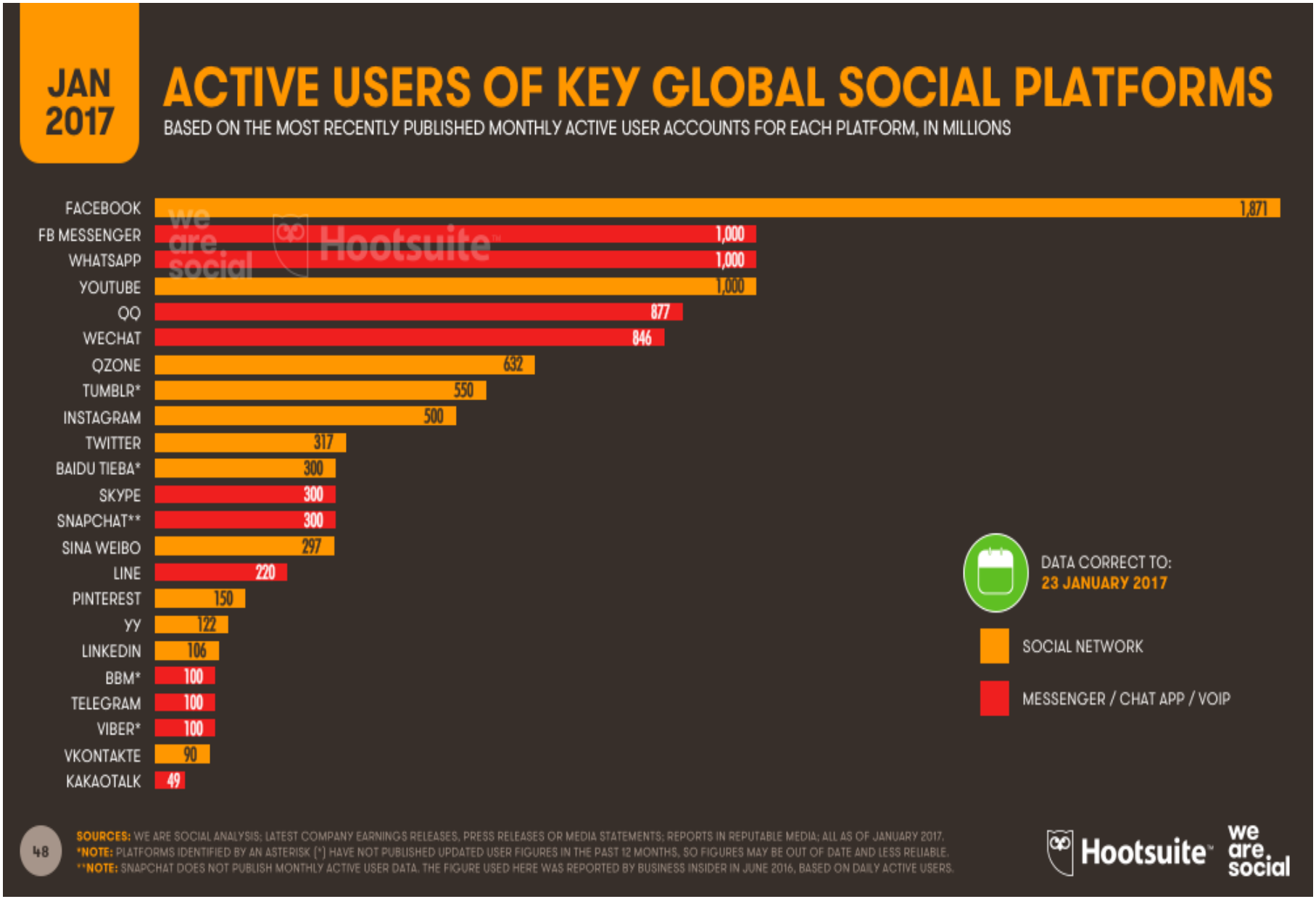
Roma, 25 novembre 2017


SURFACE WEB
Google
Wikipedia
Bing
Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
DEEP WEB
Multilingual Databases
Conference Proceedings
Government Resources
Competitor Websites
Organization-specific Repositories
DARK WEB
Illegal Information
TOR-Encrypted sites
Drug Trafficking sites
Private Communications



Fonte: www.wearesocial.com – report "digital 2017"

Fonte: www.wearesocial.com – report "digital 2017"



Fonte: www.wearesocial.com – report "digital 2017"

Il Phishing 1/4

Tecnica che utilizza finte *e-mail* e falsi siti *web* per sottrarre dati personali, credenziali di accesso, user-id e *password*, coordinate bancarie etc.

Spesso utilizzano *mail* di spam anche se a volte utilizzano tecniche dette di «*cross site scripting* XSS» per installare software malevolo o dirottare gli utenti;

Come funziona il *phishing*:

PHISHER

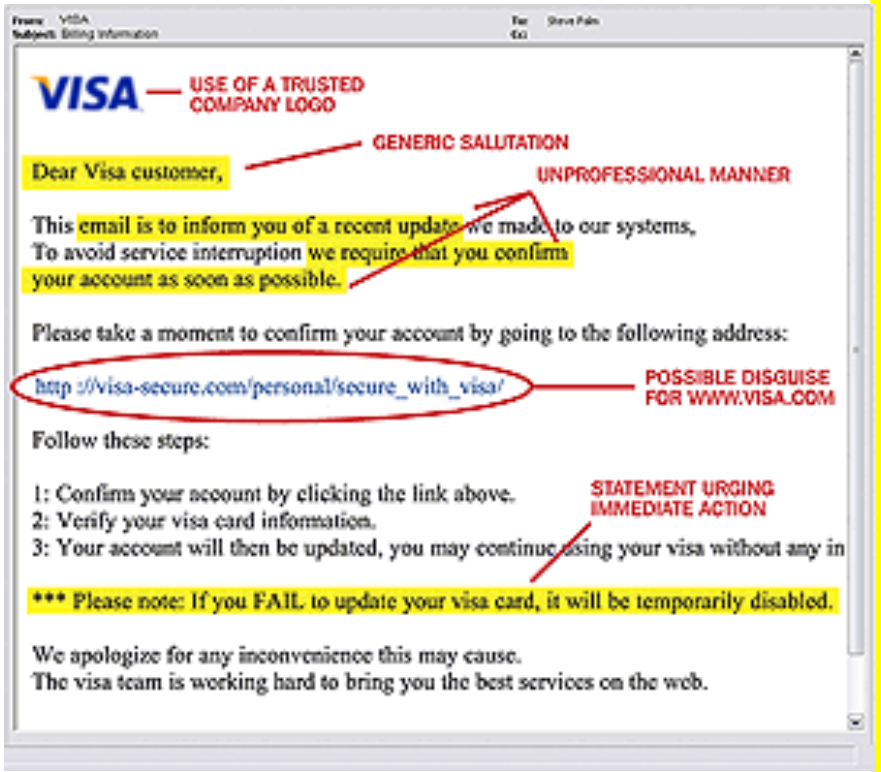
TITOLARE C/C

ASPIRANTE COLLABORATORE

Il Phishing 2/4

Come funziona il *phishing*:

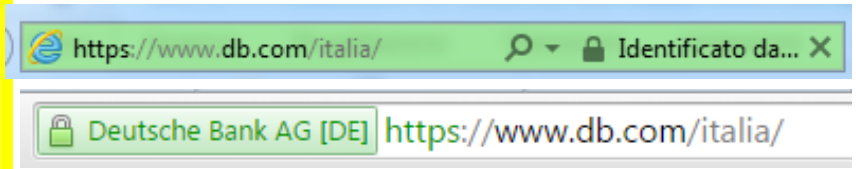
1. Il phisher invia una mail fraudolenta ad un utente invitandolo a collegarsi al sito della propria banca (oppure ad un *social network*) oppure ad aprire un allegato.

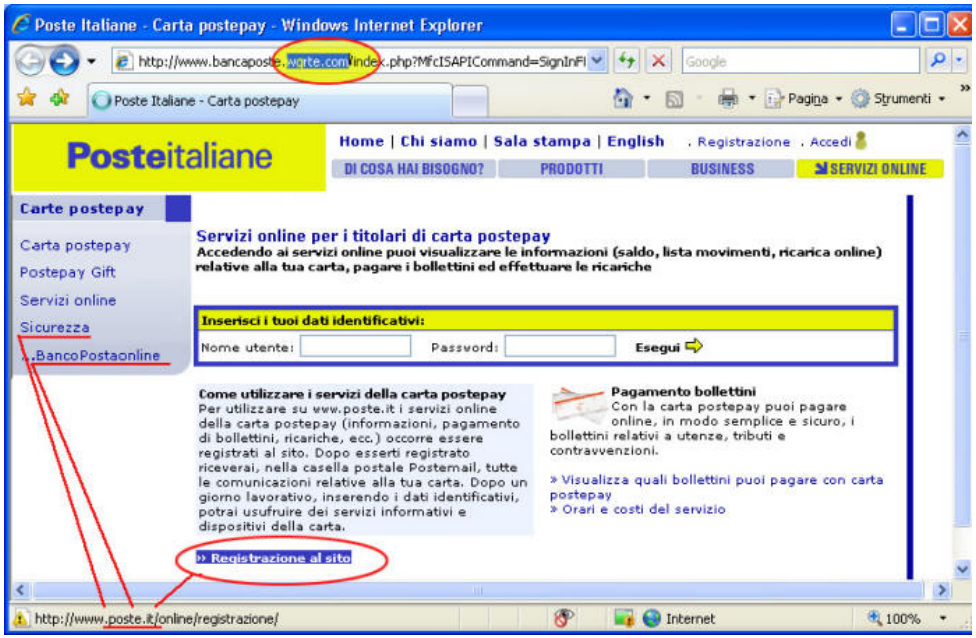


Il Phishing 3/4

Come funziona il *phishing*:

2. l'utente viene dirottato verso un finto sito di un istituto di credito o *social network*…. ed inserisce le proprie credenziali;



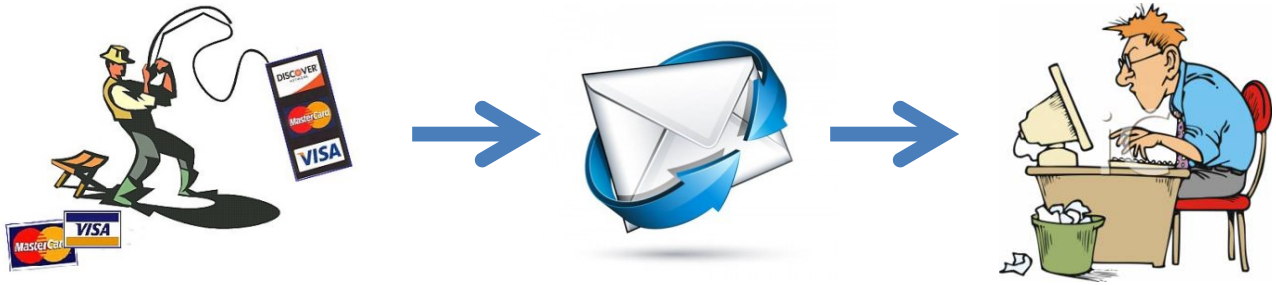


Il Phishing 4/4

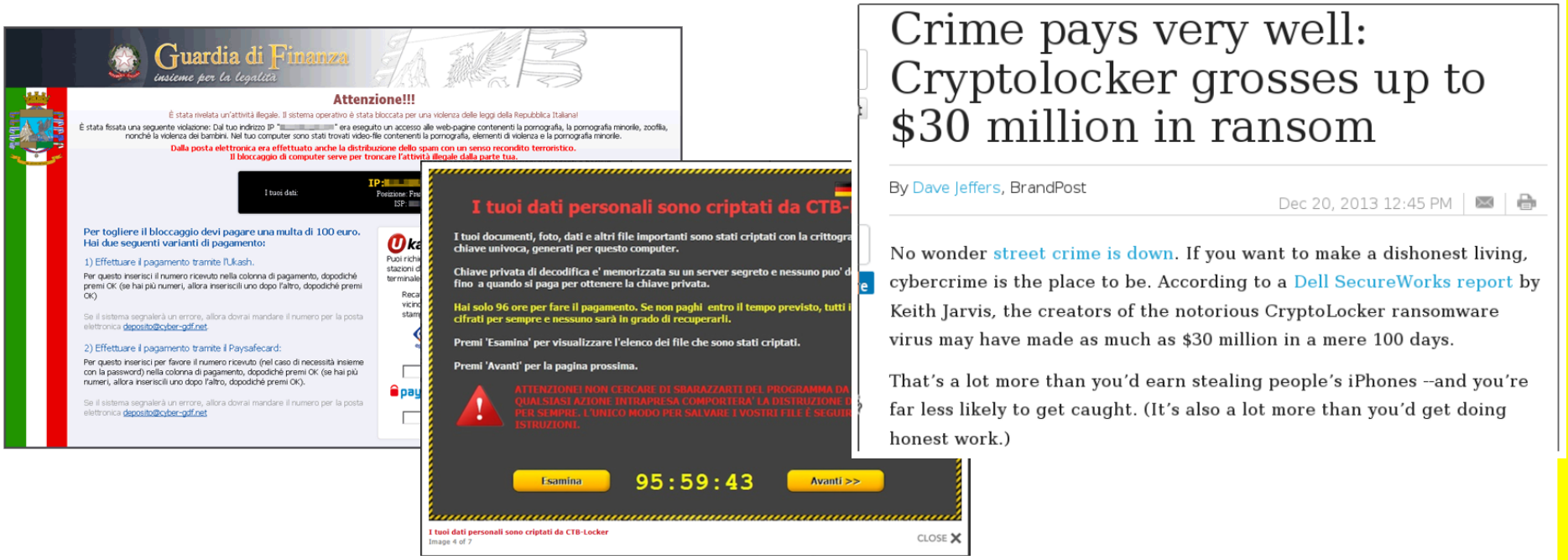
Come funziona il *phishing*:

3. il *phisher* non può effettuare bonifici sul suo conto corrente, altrimenti sarebbe subito smascherato. Invia quindi una mail contenente una falsa offerta di lavoro a domicilio ad un soggetto terzo… chi risponde non dovrà far altro che indicare il proprio IBAN ed essere disponibile a ricevere dei bonifici.

   Parte di quanto riceve lo dovrà inviare a soggetti terzi attraverso agenzie di *money transfer*, e lui si terrà una piccola percentuale a titolo di commissione



I Ransomware



I Social Network

I social network hanno cambiato il concetto di amicizia del XXI secolo… ci sono persone che hanno migliaia di amici…

Più «amici» si hanno e più si è esposti al problema del furto di identità online

Ma cos'è un amico?

Numero di Dunbar

Da Wikipedia, l'enciclopedia libera.

Il **numero di Dunbar** è una quantificazione numerica del limite cognitivo teorico che concerne il numero di persone con cui un individuo è in grado di mantenere relazioni sociali stabili, ossia relazioni nelle quali un individuo conosce l'identità di ciascuna persona e come queste persone si relazionano con ognuna delle altre.[1][2][3][4][5][6]

Le stime sul valore del numero di Dunbar, in realtà, oscillano tra 100 e 250, ma l'approssimazione adoperata di solito è 150.

1997

partendo dalla teoria dei "6 gradi di separazione",
nasce il primo social network

- **oltre 200 social network**
- **circa 40 portali specializzati in incontri**

I social media possono essere suddivisi in:

- ✓ *profile-based*
- ✓ *content-based*
- ✓ *entertainment*
- ✓ *business*
- ✓ etnici/comunità
- ✓ *blog-based*
- ✓ *micro-blogging*
- ✓ tematici
- ✓ *mobile*

Social network, un’opportunità per le aziende….

…. ma anche per le organizzazioni criminali

Attenzione a ciò che si pubblica….

…ed alla propria reputazione ….

L’immaterialità della “piazza virtuale” amplifica le disinibizioni, le volgarità e le condotte illecite

- **sexting**
- **stalking**
- **cyberbullismo**
- **diffamazione**

Libero - 15 dicembre 2016

La statistica di una società di allarmi

Tre ladri su quattro usano i social per scegliere le case da razziare

I banditi controllano su Facebook, Instagram e Twitter la disponibilità economica e i movimenti delle potenziali vittime. Ecco quali regole seguire per tenerli alla larga

GIANLUCA VENEZIANI

Oggi anche il Kevin di "Mamma ho perso l'aereo", anziché manichini, trappole e voci di film registrati per scacciare via i ladri, prenderebbe le adeguate contromisure sui social network. I ladri non sono più quella coppia di scalcagnati malviventi che attentano a casa McCallister, ma si sono aggiornati a livello tecnologico e utilizzano Facebook, Twitter o Instagram per portare a termine i loro furti: rubano informazioni alle vittime per poi rubare oggetti nelle loro case.

Come rende noto Verisure, società leader in Europa nel mercato degli allarmi, addirittura il 75% dei ladri - vale a dire tre su quattro - si avvale dei social per identificare le potenziali vittime, capire cosa possiedono, dove vivono e quanto tempo trascorrono

scaccia-ladri. Ecco qua alcuni consigli utili. In primis, è bene non condividere sui social informazioni personali come la via di casa, il posto di lavoro e il proprio numero di telefono. In secondo luogo, è preferibile evitare di postare in tempo reale su Facebook, Twitter o Instagram le foto dei propri viaggi: il che non vuol dire autocensurare per paura ogni immagine di vacanza, ma pubblicarla in modo intelligente nel momento in cui si torna a casa (magari varrà qualche "like" in meno postarla l'8 gennaio, ma si guadagna in tranquillità). In terzo luogo, sarebbe bene disattivare sui social la geolocalizzazione, che spesso viene inserita automaticamente. Così come impostare la privacy in modo che solo gli amici possano vedere qu... pubblic...

gioco facile per svaligiare le abitazioni (in un rovesciamento simbolico inquietante per cui sottraggono cose anziché portare doni, come fanno le persone perbene). Altri dati Verisure relativi al 2015 dimostrano infatti che nel mese di dicembre i furti raddoppiano rispetto alla media dell'anno, con una percentuale del 14% sul totale annuo rispetto al 7-8% degli altri mesi. E questo in un contesto in cui la paura di essere derubati cresce insieme alla sensazione generale di pericolo. Un sondaggio condotto dall'istituto Sondea nel 2016 conferma che un italiano su due teme un'intrusione in casa e ben 8 italiani su 10 co... scono un amico o un... re che ha subit...

VareseNews

VareseNews

http://www.varesenews.it

Occhio al post: ladri in agguato su Facebook

Data : 18 agosto 2016

L'ultima frontiera dei furti in appartamento durante la stagione estiva sono i **social network.** «Sono sempre più i ladri, stando ai dati divulgati dalle Forze dell'Ordine, che scelgono di monitorare gli **spostamenti delle future vittime su Facebook**, onde agire indisturbati sapendo di trovare con certezza l'abitazione libera».

Lo dichiara l'avvocato Patrizia Polliotto, Fondatore e Presidente del Comitato Regionale del Piemonte dell'Unione Nazionale Consumatori, dal 1965 a oggi la più antica e autorevole associazione consumeristica italiana.

raccomandazione è quella, per i consumatori, di non scrivere o pubblicare post su ... o sui comuni social network, in cui si danno informazioni di ogni genere legate ai ...itando di rendere noto se si è fuori casa e per quanto tempo, se in ...piega l'avvocato Polliotto.

...tenere sempre gli occhi ...e le chiavi

POSSIBILI RIMEDI

Il primo accorgimento da adottare è leggere accuratamente il codice di condotta e le regole applicate sul trattamento dei dati da parte del social network…

… sarà poi necessario:

POSSIBILI RIMEDI

- ✓ **utilizzare di password “robuste”**
- ✓ **porre attenzione alle impostazioni della privacy del proprio profilo**
- ✓ **verificare i dettagli delle fotografie pubblicate (EXIF)**
- ✓ **evitare l’uso di dati identificativi completi**
- ✓ **considerare cosa viene pubblicato e gli effetti che potrebbe assumere nel tempo**

… sarà poi necessario:

POSSIBILI RIMEDI

- ✓ **riflettere sul fatto che di ogni contenuto che si immette in Rete, se ne perde il controllo, rendendolo di fatto “immortale”**
- ✓ **non sottovalutare la rilevanza professionale del proprio profilo personale**
- ✓ **pubblicare informazioni attinenti alle vacanze o viaggi di lavoro soltanto a posteriori**
- ✓ **mantenere il proprio PC ed antivirus aggiornati**

… e per concludere….

"If you are not paying for it, you're not the customer; you're the product being sold."

Grazie
per l’attenzione