SUPSI

Cyber criminalità, evoluzione e modus operandi

Come pensa un hacker

Dr.-Ing.- Alessandro Trivilini, Ph.D.

www.trivilini.info

18.11.2017

EVOLUZIONE DEL CYBERCRIME

La realtà: “security is an illusion”

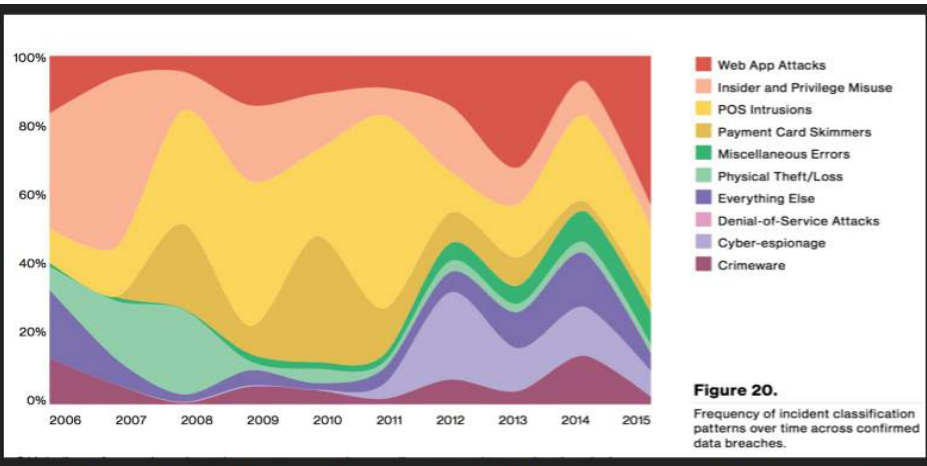
www.kaspersky.com

<<2016 was the year when “sooner or later” became “now”>>

È solo una questione di tempo e il proliferare di attacchi informatici di ultima generazione, sempre più resilienti, colpirà nel 2017 un numero crescente di piccole e medie aziende sfruttando l’anello più debole della sicurezza informatica:

il **fattore umano**.

Tipologia e tendenza dei cyber attacchi



FREQUENCY OF INCIDENT CLASSIFICATION PATTERNS OVER TIME ACROSS CONFIRMED DATA BREACHES.
VERIZON DATA BREACH INVESTIGATIONS REPORT (2016)

Fonte: Jeremiah Grossman, BlackHat, Las Vegas, 2016

EUROPOL – Piattaforma SIRIUS

www.europol.europa.eu

SIRIUS is a secure web platform for law enforcement professionals, which allows them to share knowledge, best practices and expertise in the field of internet-facilitated crime investigations, with a special focus on counter-terrorism. It offers an innovative collaborative approach by providing investigators with a platform to quickly and efficiently exchange know-how, manuals and advice, as well as tools to help them analyze the information received by the different online service providers.

IL FATTORE UMANO E IL CYBERCRIME

DATA BREACHES

È la trasmissione non autorizzata di informazioni sensibili ad una terza parte non è autorizzata a possedere o vedere l'informazione (es. Sony, Yahoo, etc ..)

PHISHING

Ê un tipo di truffa attraverso la quale (e-mail e siti web) si cerca di ingannare la vittima a fornire informazioni personali e/o aziendali (es: dati finanziari, password, etc.) fingendosi un contatto affidabile e fidato.

Pensare come un Hacker

Questo e-mail è stato spedito da un collega, amico o qualcuno che conoscco personalmente?

L'orario di ricezione dell'email è quello ordinario, per I contenuti e attività, oppure no?

Nel messaggio e-mail che ho ricevuto mi viene chiesto di premere un un link particolare esterno oppure di scaricare un allegato, oppure di disiscrivermi da un servizio promozionale?

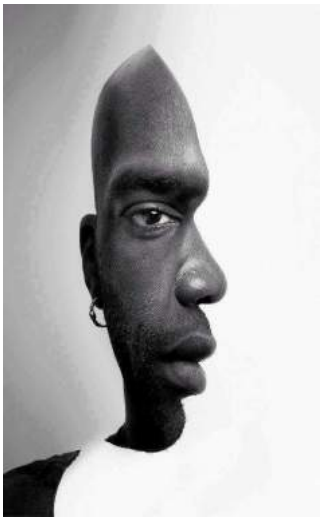
Ho ricevuto un e-mail con all'interno un link contenente errori e che porta a un indirizzo web ingannevole?

Ho una relazione professioanale o personale con il mittente del messaggio?

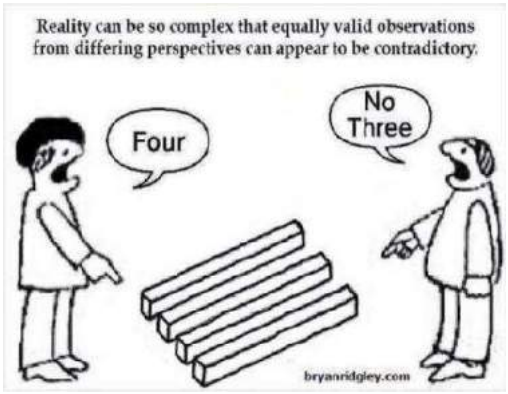
Per leggere il messaggio state usando un dispositivo personale o aziendale?

www.bankofarnerica.com Bank of America

Percezione o realtà?



Fonte: http://www.shenzhenstuff.com



Fonte: http://www.infusefive.com

Affordances

"The ecological approach to visual perception"
J. Gibson, 1979

It is a **quality** of an object, or an environment, that allows an individual to perform an action.

All "action possibilities" latent in the environment, objectively measurable and independent of the **individual's ability** to **recognize** them.

Design feature that helps thinking and/or knowing about something (In a button label could be a **cognitive affordance** enabling users to understand the meaning of the button in terms of the functionality behind the button and the consequences of clicking on it.

emozioni **memoria** **attenzione** **linguaggio** **percezione** **apprendimento**

3 (fatidici) secondi di tempo!

Similarity

Nello stesso ambiente gli elementi tra loro simili per **forma**, **colore** e **dimensione** vengono percepiti come collegati

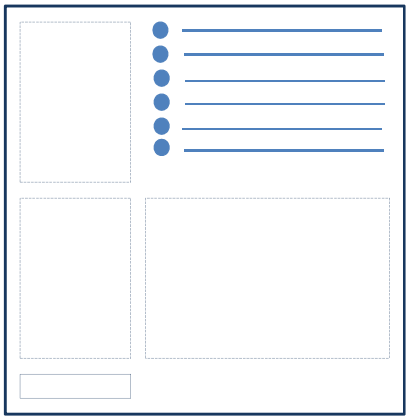
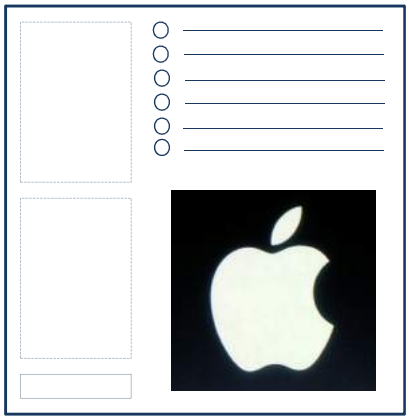


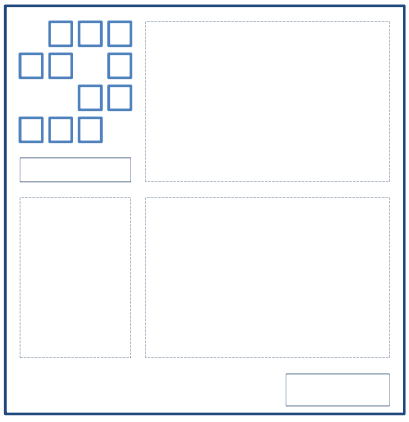
Figure & Background

Le figure vengono percepite prima di tutto dal proprio **contorno**, il resto viene inteso come **sfondo** (appartenenza, è parte di ..)



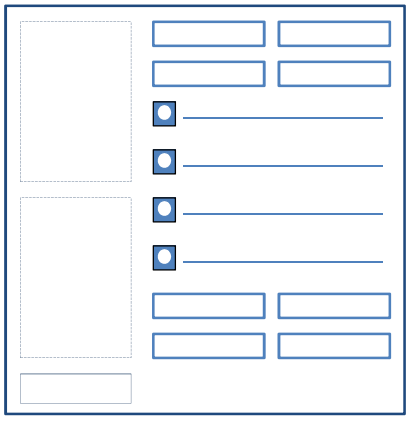
Closure

Linee e forme familiari vengono percepite come **chiuse** e **complete**, anche se graficamente non lo sono



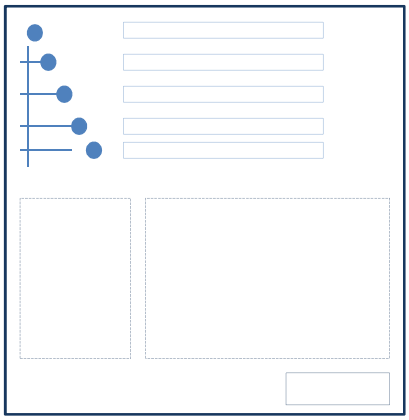
Proximity

All'interno di una stesso ambiente gli elementi tra loro **vicini** vengono percepiti come un tutto (intero e le sue parti …)



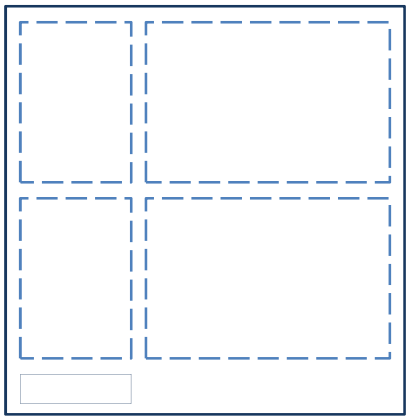
Continuity

Elementi posizionati linearmente vicini uno all'altro porta lo sguardo (**percezione**) a **proseguire** lungo e oltre una linea retta o una curva.



Simmetry

Se un oggetto può essere diviso in due metà più o meno **simmetriche**, la **percezione** che ne risulta è di considerare le due parti simmetriche appartenenti allo **stesso** oggetto (**intero**)



IL PHISHING & IL RANSOMWARE

Il primo contatto!

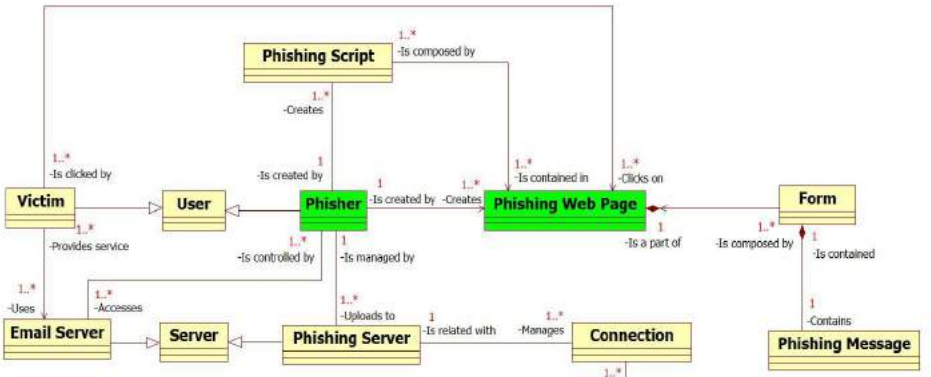
L'**e-mail** è il **vettore** più utilizzato per veicolare in rete virus e captatori (trojans) per il furto dei dati digitali e la violazione delle infrastrutture critiche aziendali.

Come riconoscerli?

1) Controllare le informazioni del mittente
2) Verificare i link sospetti ("unsubscribe" compresi) con il "mouse over" per verificare l'effettiva destinazione
3) Controllo della grammatica/linguaggio del testo del messaggio

Tecniche di social engineering per inganno percezione

Un caso reale: il Phishing



Furto indentità (e-mail)!
Keylogger (hardware)
Spunta login automatici
Brute forcing

“Security is an illusion e Dave è ovunque!

Human behavior is (very) predictable!

Grazie.

Dr.-Ing.- Alessandro Trivilini, Ph.D.

www.trivilini.info