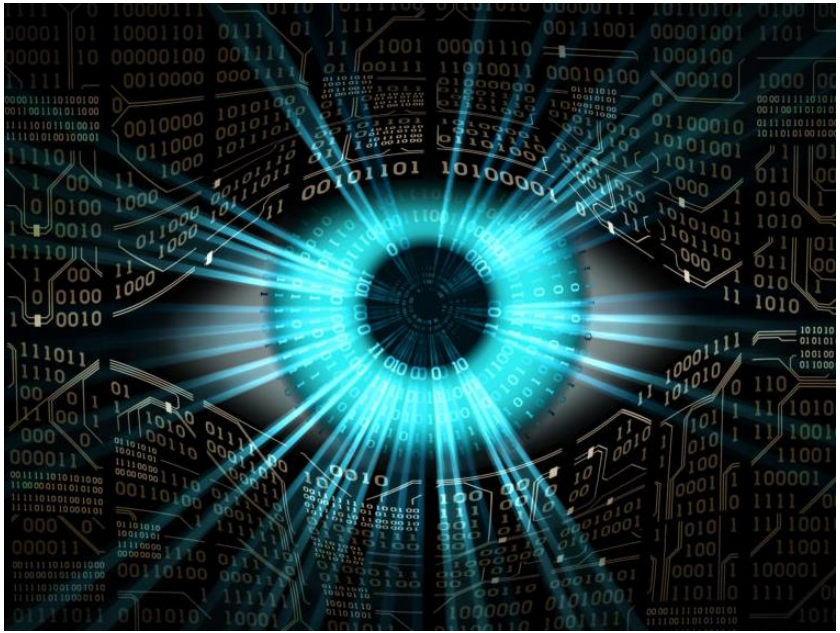
SCUOLA DIGITALE LIGURIA

Safer Internet Day



Minacce online e cyber security: navigare consapevolmente si può

Massimiliano Balistreri

system engineer & digital team
Liguria Digitale s.p.a.

Liguria Digitale

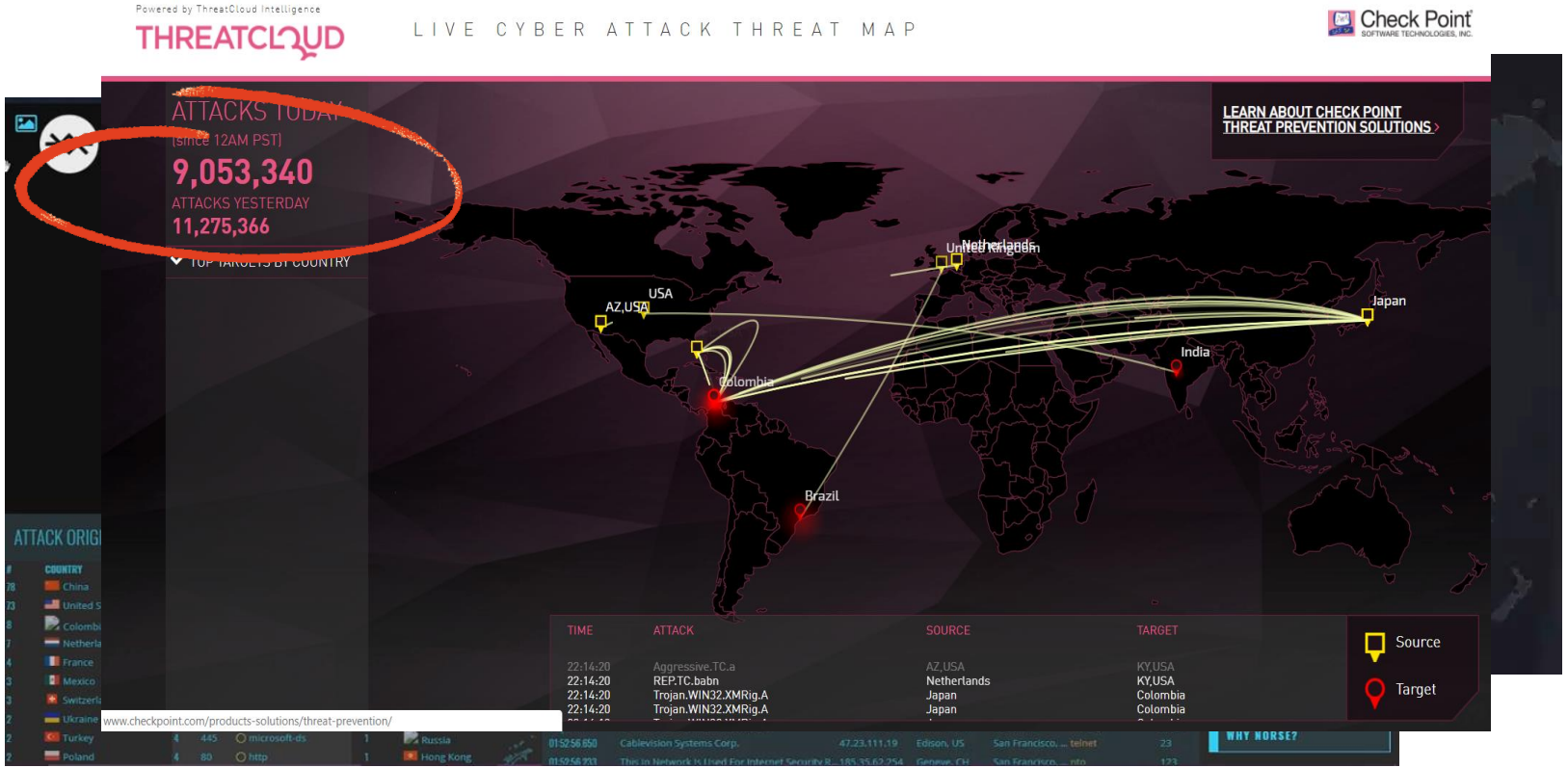
REGIONE LIGURIA

In un minuto su internet nel mondo…

Nel frattempo…

Nel frattempo…

PROGETTO SCUOLA DIGITALE LIGURIA



Nel frattempo…

REGIONE LIGURIA

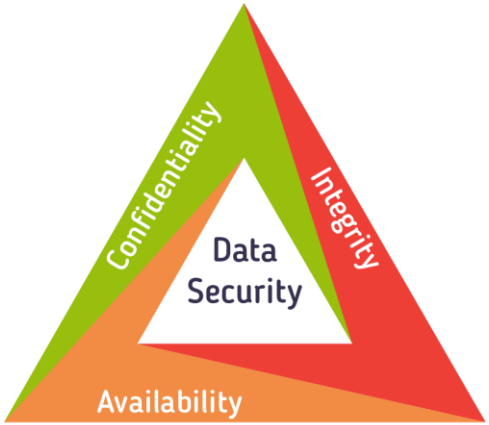
Liguria Digitale

Che significa avere un dato sicuro?

La **sicurezza informatica** è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di:

- **Riservatezza**: accesso ai dati ai soli soggetti autorizzati;
- **Integrità**: dati completi e non alterati;
- **Disponibilità**: accessibilità dei dati e dei servizi quando è necessario.

- Riservatezza
- Integrità
- Disponibiltà

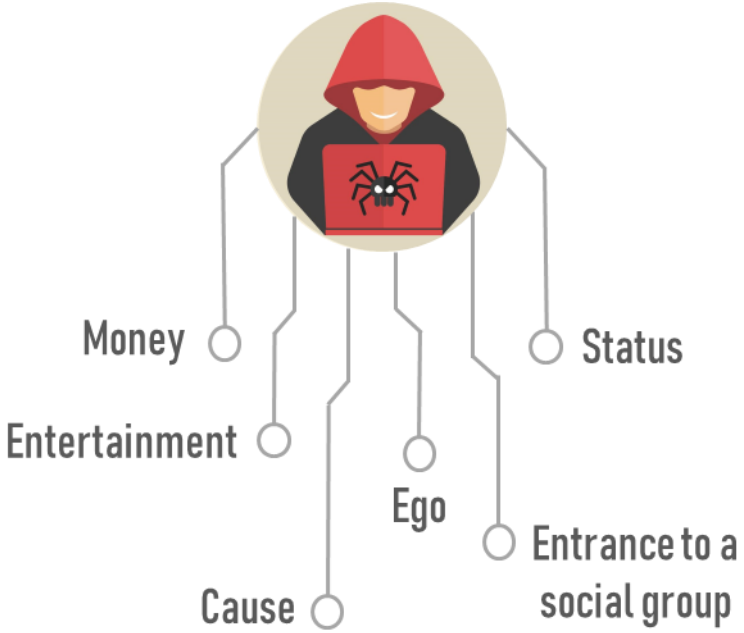


Gli attori in gioco

Attaccanti

- Script kiddie
- Cybercrime
- Cyber soldiers
- Cyber terrorism
- Hacktivist

Motivazioni



Gli attori in gioco

Bersagli

AZIENDE PUBBLICHE E PRIVATE

PERSONE

ORGANI GOVERNATIVI E MILITARI

OPERATORI DI SERVIZI ESSENZIALI

- Energia (elettricità, petrolio, gas)
- Trasporti (ferroviari, aerei, vie d'acqua)
- Banche e società finanziarie
- Salute (ospedali, cliniche private)
- Acqua (fornitura e distribuzione)
- Infrastrutture digitali (IXP, DNS, TLD)

SOCIAL ENGINEERING: IL PROLOGO DI UN ATTACCO

Tecniche di **manipolazione psicologica** per indurre le persone a svolgere determinate azioni o a divulgare informazioni riservate.
Spesso rappresenta la prima parte di un attacco:

- raccolta di informazioni
- frodi
- Informazioni di accesso a sistemi, etc…

Kevin Mitnick, hacker e autore de *L'arte dell'inganno*

Modalità di azione

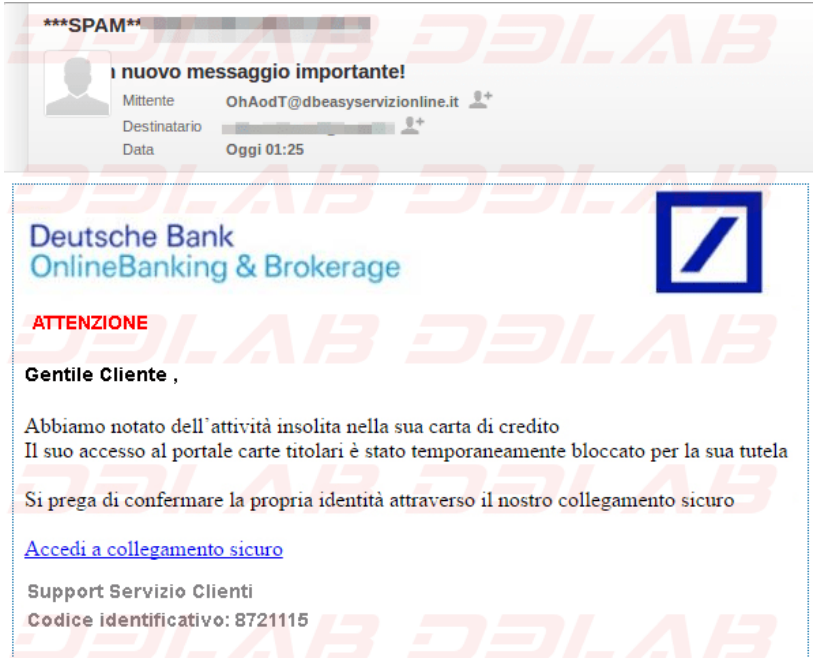
- Raccolta di informazioni sulla vittima (osint, humint…)
- Creazione di un pretesto (falsa ambientazione che coinvolga la vittima)
- Esecuzione

DAL SOCIAL ENGINEERING AL PHISHING

Tecnica di social engineering per ottenere informazioni personali, dati finanziari o codici di accesso attraverso comunicazioni elettroniche che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi.

- SPAM
- PHISHING
- SPEAR PHISHING
- WHALING «caccia alla balena»

PHISHING CONTRO PRIVATI



***SPAM**

nuovo messaggio importante!

Mittente OhAodT@dbeasyservizionline.it

Destinatario

Data Oggi 01:25

Deutsche Bank
OnlineBanking & Brokerage

ATTENZIONE

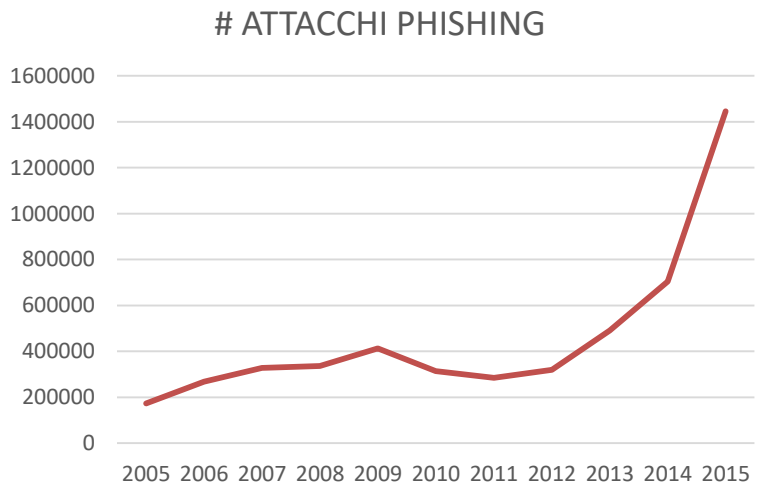
Gentile Cliente ,

Abbiamo notato dell'attività insolita nella sua carta di credito
Il suo accesso al portale carte titolari è stato temporaneamente bloccato per la sua tutela

Si prega di confermare la propria identità attraverso il nostro collegamento sicuro

Accedi a collegamento sicuro

Support Servizio Clienti
Codice identificativo: 8721115



PHISHING TRAMITE E-MAIL BUSINESS

Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

"Sposta subito mezzo milione su questo conto estero". Ma la mail era di un hacker. E i soldi sono spariti. Il finto ordine a firma della direttrice Panucci: "Esegui e non mi chiamare che sto fuori col presidente"

di ROBERTO MANIA

ABBONATI A Rep: 30 settembre 2017

Mail che inganna la vittima facendole credere che provenga da fonte autorevole

Mail prive di allegati o link malevoli ma contenenti richieste specifiche che spesso avvengono nelle stesse modalità

Dato FBI 2018: Tra ottobre 2013 e maggio 2018 **perdite pari a 12.536.948.299 USD** dovute a BEC

Modalità tipiche del phishing contro aziende

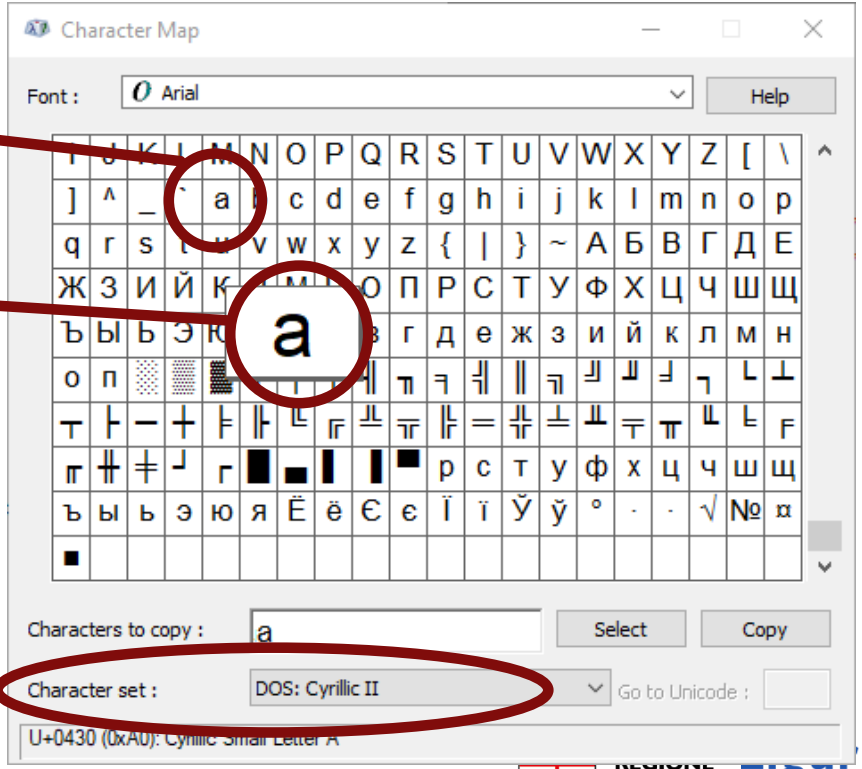
- **Studio delle comunicazioni** dell'azienda, carta intestata, firme dei responsabili, lo stile della corrispondenza, ruoli aziendali.
- Comunicazione alla persona giusta dell'azienda, coordinate bancarie diverse su cui eseguire i pagamenti e ad esempio fatture con **template uguale** a quelle vere.
- **Tecniche:**
  - accesso a casella mail violata
  - indirizzo mail molto simile all'originale: alice@liguriadigitale.it – alice@liguradigitale.it – alice@liguria-digitale.it
  - spoofing (falsificazione del mittente)

ATTACCO PHISHING DI TIPO OMOGLIFO

http://www.finanze.it

http://www.finanze.it

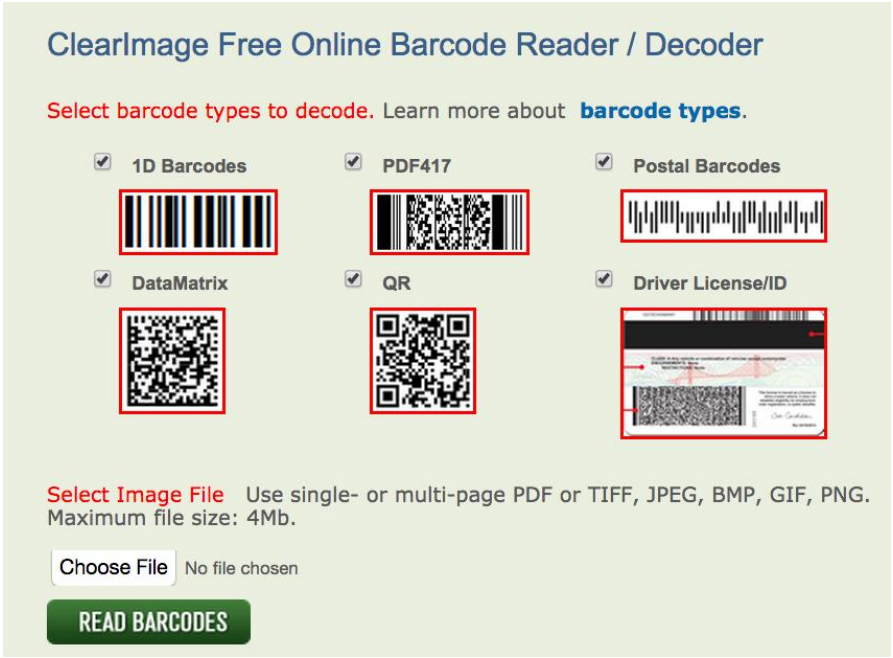
http://www.xn--finnze-5nf.xn--t-c9h/



Questo tipo di attacco non è più facilmente attuabile poiché viene identificato dai browser

ESEMPIO DI UNA COSA CHE NON BISOGNA FARE

RISCHI NELL'USO DEI SOCIAL NETWORK



https://online-barcode-reader.inliteresearch.com/default.aspx

The next step was to try a real boarding pass issued at the airport.

M1EWING/SHAUN E1AAAAA SYDBNEQF 0524 106Y023A0073 359>2180
B 29 0 QF 1245678 128
There's more information in this boarding pass barcode, which is as follows:

M1: Format code 'M' and 1 leg on the boarding pass.
EWING/SHAUN: **My name.**
E1AAAAA: Electronic ticket indicator and my booking reference.
SYDBNEQF: Flying from SYD (Sydney) to BNE (Brisbane) on QF (Qantas).
0524**: Flight number 524.**
106: The Julian date. In this case 106 is April 16.
Y: Cabin – Economy in this case. Others including F (First) and J (Business).
23A: My seat.
0073: My sequence number. In this case I was the 73rd person to check-in.
3: **My "passenger status".**
59: There is a various size field. This is the size
>: Beginning of the version number
2: The version number.
18: Field size of another variable field.
0: **My check-in source.**
B: Airline designator of boarding pass issuer.
2: Another variable size field.
9: Airline code.
0: International document verification. '0' as I presume is not applicable.
QF: **The airline my frequent flyer account is with.**
1245678: **My frequent flyer number.**
128: Airline specific data.

ALCUNE SEMPLICI REGOLE PER DIFENDERSI:

- Verificare l'attendibilità dei siti, in particolare da cui si acquista (SSL)
- Usare solo sistemi di pagamento sicuri e tracciabili (bonifico, Paypal, carte di credito)
- Tenere il sistema operativo ed il browser aggiornati
- Installare un antivirus e aggiornarlo

Essere prudenti e dotarsi di buon senso

PER PREVENIRE E DIFENDERSI: NUOVE OPPORTUNITÀ DI LAVORO

La crescita del mondo connesso va di pari passo con le occasioni di hacking, spingendo le aziende a creare nuovi settori al loro interno dedicati al security management.

In Liguria Digitale il team che si occupa di cyber security conta su una decina di elementi, tra dipendenti e tirocinanti. Ed è in continua espansione.

Unione europea
Fondo sociale europeo

Repubblica Italiana

REGIONE LIGURIA

SCUOLA DIGITALE LIGURIA

www.scuoladigitaleliguria.it

Progetto Scuola Digitale Liguria

scuoladigitale@regione.liguria.it