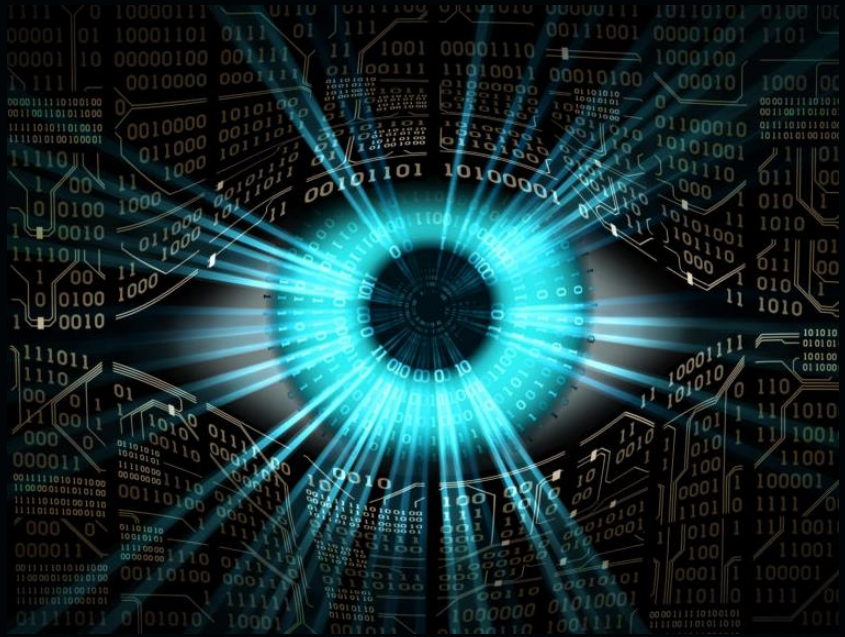
Unione europea
Fondo sociale europeo

Repubblica Italiana

REGIONE LIGURIA

Liguria Digitale

SCUOLA DIGITALE LIGURIA



ORIENTAMENTI SUMMER

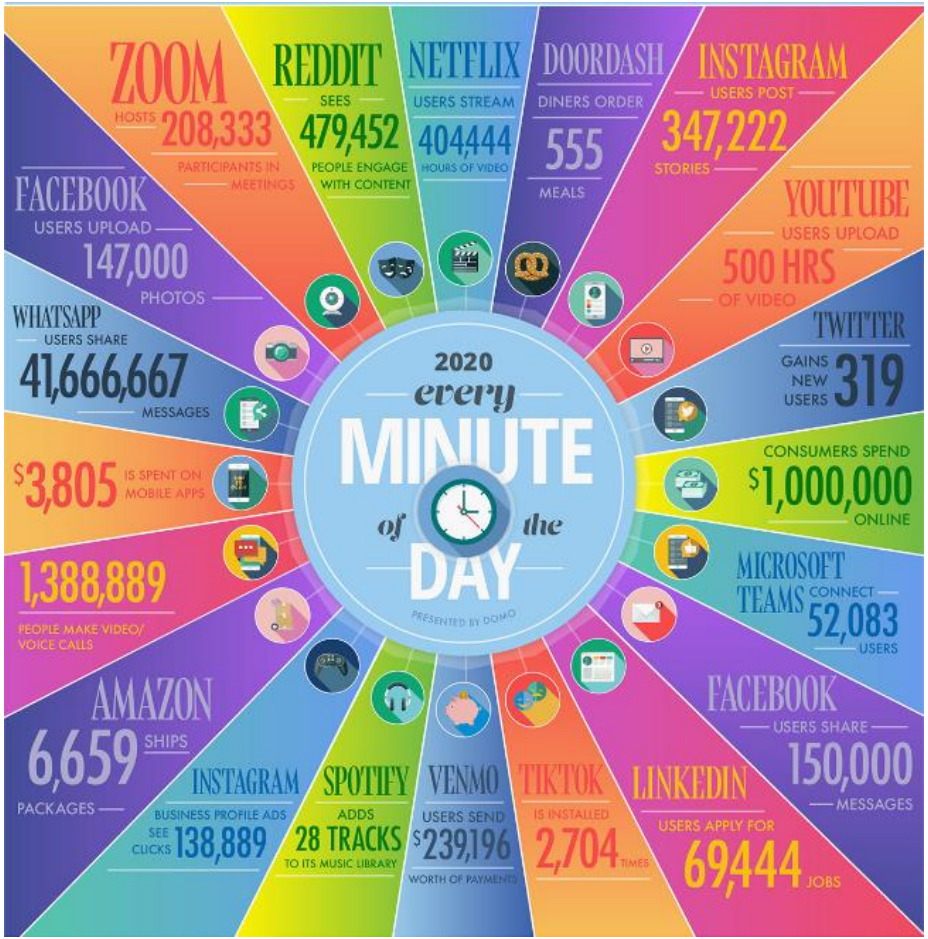
Minacce online e cyber security: navigare consapevolmente si può

Massimiliano Balistreri
(System engineer - Liguria Digitale, Digital Team)

13/14/15 luglio 2021

digitalteam@regione.liguria.it

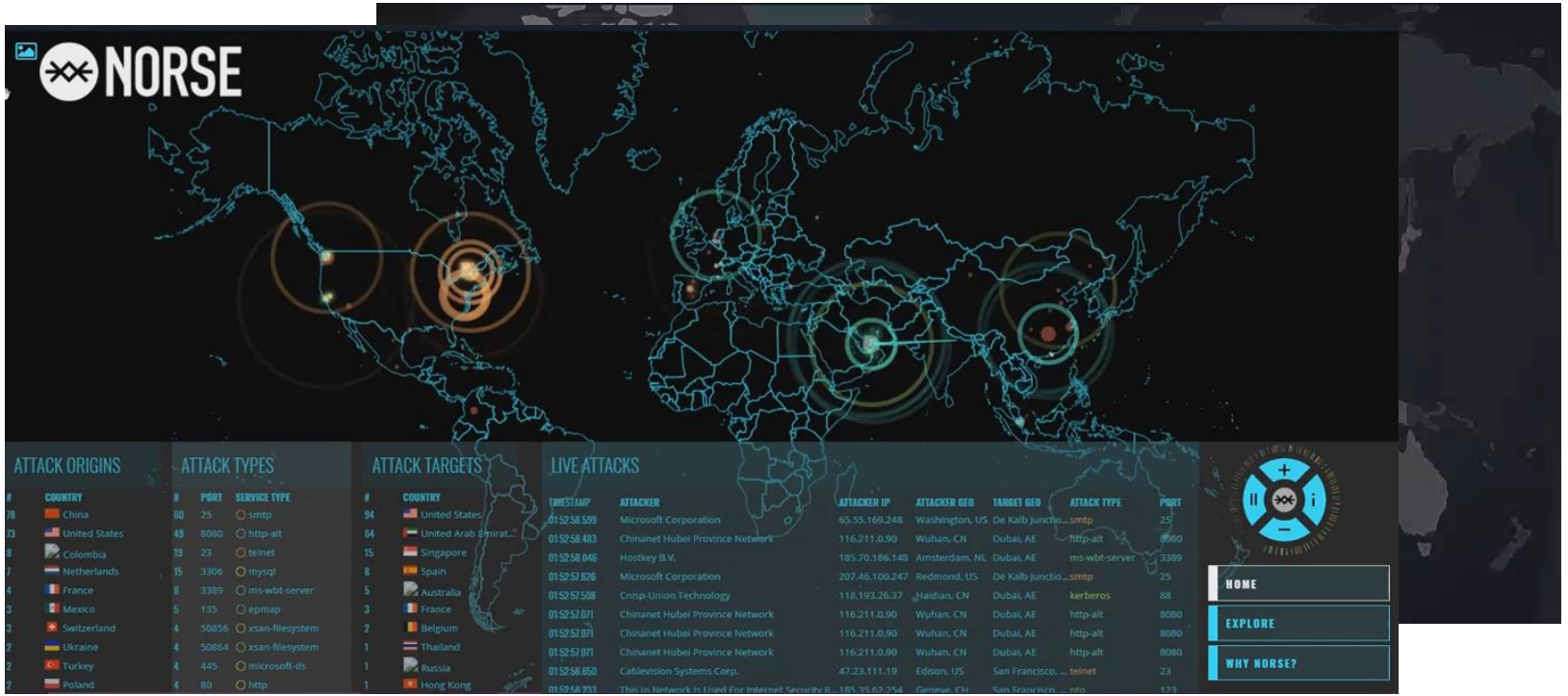
IN UN MINUTO SU INTERNET NEL MONDO…



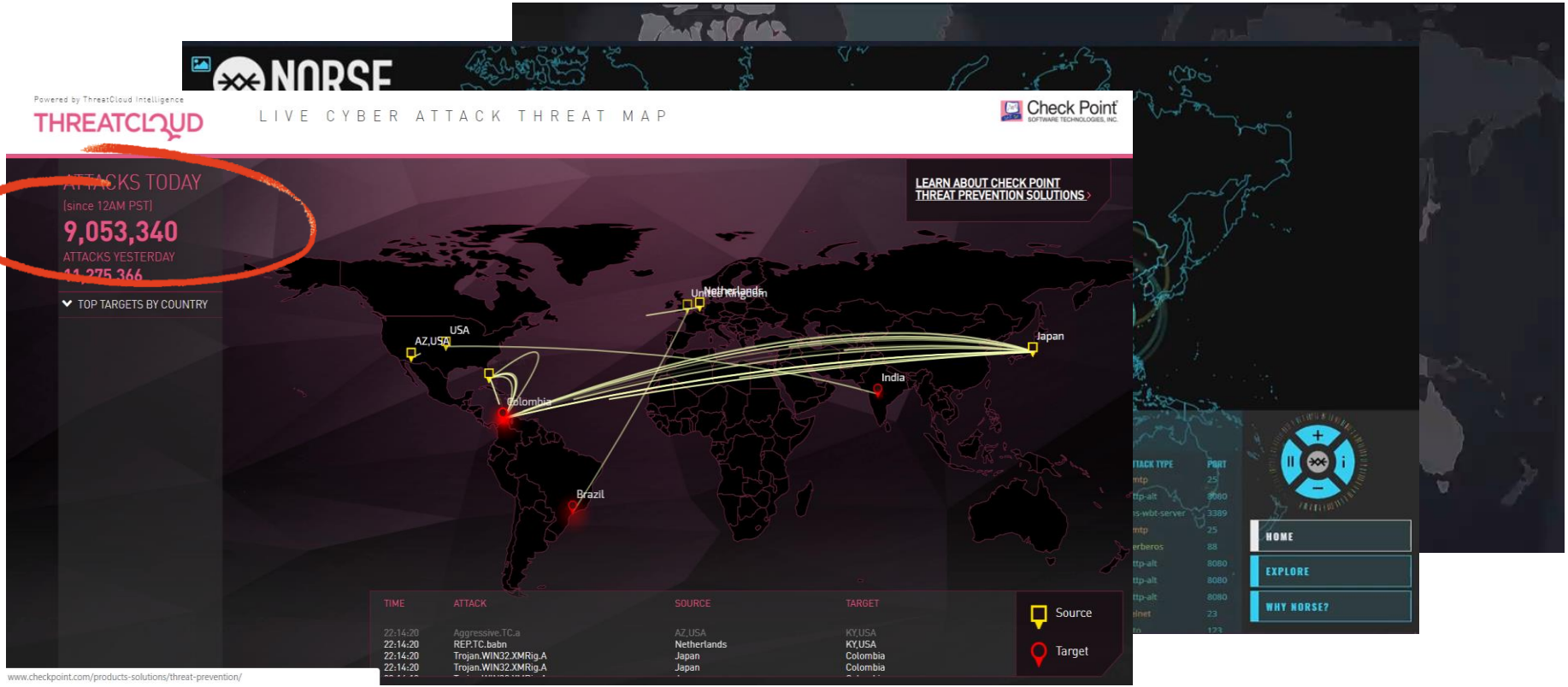
https://www.domo.com/learn/infographic/data-never-sleeps-8

NEL FRATTEMPO…

NEL FRATTEMPO…



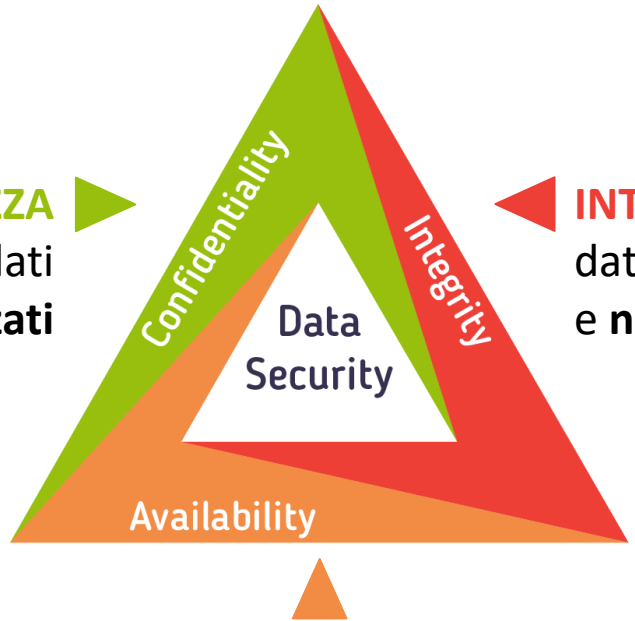
NEL FRATTEMPO…



COSA VIENE ATTACCATO? I NOSTRI DATI

La **sicurezza informatica** è la disciplina che studia e applica i metodi per proteggere i nostri dati.
I sistemi che gestiscono i nostri dati sono sicuri quando garantiscono:

RISERVATEZZA
accesso ai dati
ai soli soggetti autorizzati



INTEGRITÀ
dati completi
e **non alterati**

DISPONIBILITÀ
accessibilità dei dati e dei servizi **quando è richiesto**

TUTTE LE NOSTRE AZIONI IN RETE HANNO CONSEGUENZE

- Ogni contenuto condiviso sui social (una foto, un video o un semplice like) rimane in rete
- Le tracce che lasciamo nella navigazione web (i cookies) possono essere collezionate ed archiviate
- I nostri profili digitali diventano preziosi per chi vuole venderci qualcosa o attaccarci a scopo di estorsione

Internet spesso ci conosce meglio di chiunque altro

I DATI CHE CONDIVIDIAMO VOLONTARIAMENTE…

- Carta d’identità
- Targa della macchina
- Informazioni mediche
- Coordinate geografiche
- Biglietti (aereo, concerti, …)

Il video che ora vi mostrerò racconta una realtà forse non troppo lontana da noi:

I NOSTRI DATI IN RETE FANNO GOLA AI MALINTENZIONATI

- Internet è come l'oceano: un luogo in apparenza tranquillo di cui spesso conosciamo solo la superficie ma che nasconde nelle sue profondità realtà che sfuggono alla nostra primaria percezione.
- Come l'oceano può essere pericoloso se affrontato con leggerezza così la rete può farci male se ignoriamo i principi basilari per difenderci.

CHE COSA PUO' SUCCEDERCI NAVIGANDO SENZA REGOLE?

Diventiamo Bersagli

AZIENDE PUBBLICHE E PRIVATE

PERSONE

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)

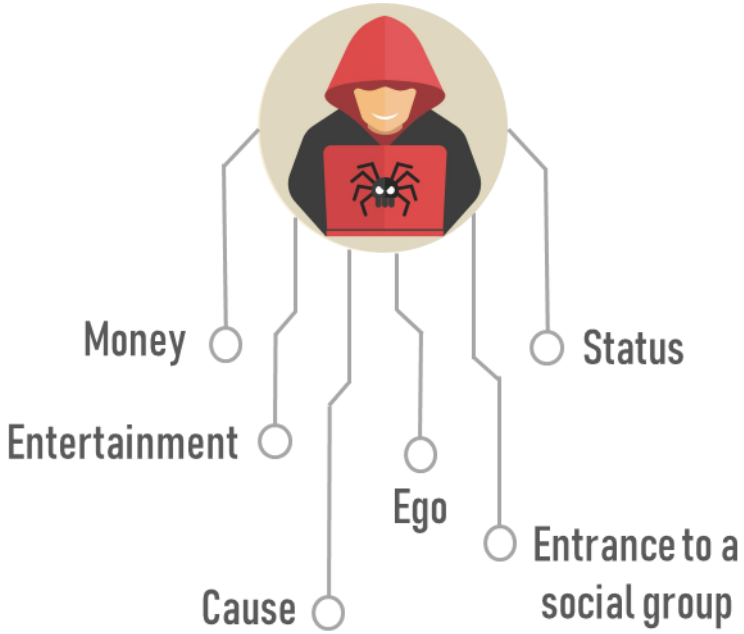
ORGANI GOVERNATIVI E MILITARI

GLI ATTORI IN GIOCO

Attaccanti

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

Motivazioni



SOCIAL ENGINEERING: IL PROLOGO DI UN ATTACCO

Si tratta di tecniche di **manipolazione psicologica** per indurre le persone a svolgere determinate azioni o a divulgare informazioni riservate.

Spesso rappresentano la prima parte di un attacco:

- la raccolta di dati personali
- frodi
- credenziali di accesso a sistemi, etc…

Modalità di azione

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

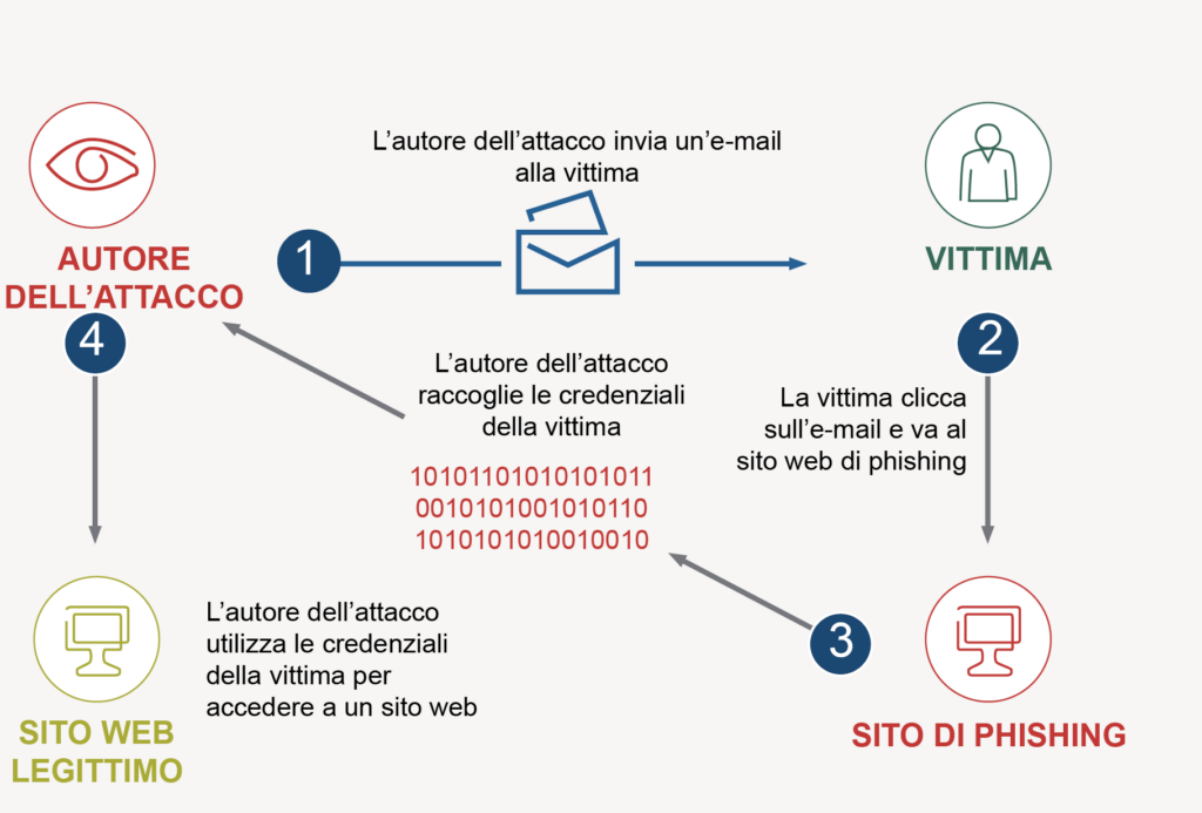
Kevin Mitnick,
hacker e autore de
L'arte dell'inganno

DAL SOCIAL ENGINEERING AL PHISHING

Le tecnica di social engineering servono ad ottenere informazioni personali, dati finanziari o codici di accesso attraverso comunicazioni elettroniche che imitano, nell'aspetto e nel contenuto, messaggi di legittimi di fornitori di servizi (e-mail, SMS, messaggi su social)

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

PHISHING CONTRO PERSONE

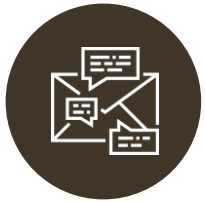


- Il phishing riguarda tutti noi (attacchi massivi)
- Gli autori dell'attacco non conoscono le vittime ma pescano nel mucchio
- Il phishing non ci colpisce solo via e-mail ma anche tramite SMS, messaggi sui social network (Whatsapp, Facebook, etc.)
- Nessuno può ritenersi immune da tentativi di attacco

Fonte: https://www.enjoysystem.it/phishing-come-evitare-truffe-online/

COME ACCORGERSI DI UNA MAIL PHISHING:
controlla il mittente, cerca l'errore

- Controllare il mittente delle e-mail e assicurarsi che sia attendibile (spoofing)
- Valutare i testi dei messaggi, che spesso contengono errori perché tradotti da strumenti automatici



- Allegati inattesi nascondono pericoli (Ransomware)
- La fretta è cattiva consigliera (premi da ritirare o pagamenti bloccati ci spingono ad agire prima di pensare)

- Su internet nessuno regala nulla (vincite incredibili o oggetti in vendita a prezzi stracciati spesso nascondono insidie)

10 SEMPLICI REGOLE PER DIFENDERSI:

- ✓ Limitare la diffusione dei nostri dati personali (social, siti ludici, acquisti online)
- ✓ Usare modalità anonime quando non siamo sicuri dei siti
- ✓ Fare attenzione ad allegati e download
- ✓ Scegliere password complesse e differenziate
- ✓ Analizzare le email sospette
- ✓ 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
- ✓ Installare un anti-malware

Essere prudenti e dotarsi di buon senso

CYBER SECURITY: TANTE 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.**

Unione europea
Fondo sociale europeo

Repubblica Italiana

REGIONE LIGURIA

SCUOLA DIGITALE LIGURIA

CONTATTI

scuoladigitaleliguria.it

scuoladigitale@regione.liguria.it

digitalteam@regione.liguria.it

Gruppo e pagina “Progetto Scuola Digitale Liguria”

Canale “Progetto Scuola Digitale Liguria”