Eurizon Capital Educazione Finanziaria

La Cyber Security: riconoscerla e difendersi

In un **mondo sempre più digitale**, è fondamentale **proteggere i propri dati e compiere scelte informate**, soprattutto quando si parla di tutela di risparmiatori e investitori. Per questo, tra i temi di educazione finanziaria e cultura digitale che affrontiamo, **la cybersecurity** riveste un ruolo imprescindibile.

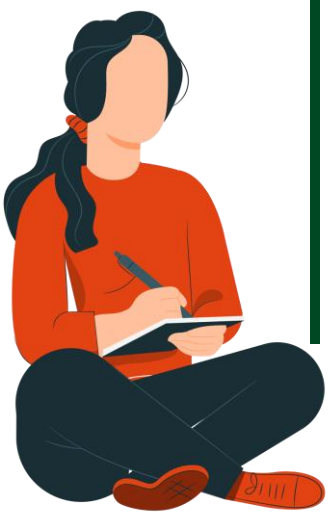
Approfondiamo insieme

EURIZON
ASSET MANAGEMENT

Indice

Conoscere i principali rischi digitali e sapere come comportarsi è fondamentale per proteggere sé stessi, i propri dati e il proprio benessere finanziario.
Vediamo insieme alcune delle **minacce più diffuse** e i **consigli per riconoscerle e difendersi**.

Ragioniamo su:



EURIZON
ASSET MANAGEMENT

Phishing: le e-mail ingannevoli

Cos'è

Si tratta di una **truffa via e-mail con l'obiettivo di rubare dati personali o confidenziali** (password, credenziali bancarie, ecc...) attraverso una call to action, ovvero una richiesta di azione

Esempio
Una e-mail che simula una conferma di pagamento da parte di una banca, contenente un allegato dannoso (.tgz). Aprendolo, si scarica un malware che ruba dati e credenziali.

Come difendersi

- **Verifica** sempre il **mittente** dell'e-mail
- **Non aprire allegati sospetti**
- **Diffida da errori grammaticali o toni allarmistici**

EURIZON
ASSET MANAGEMENT

Smishing: gli SMS truffaldini

Cos'è

Lo smishing è **simile al phishing**, ma eseguito **via SMS o app** di messaggistica. **Obiettivo**: **ottenere dati o installare malware** sul dispositivo.

Esempio
Un SMS che invita a cliccare su un link per aggiornare dati bancari o ritirare un pacco, dove il link conduce a un sito fraudolento. Vi sono numerosi casi relativi a una nuova campagna scam (truffa) dove l'SMS presenta un link che, se cliccato, invita la vittima a iscriversi a gruppi Whatsapp che propongono investimenti in criptovalute, fornendo documentazione testuale di supporto: si tratta di investimenti fittizi, utili a dirottare denaro sui conti bancari dei truffatori.

Come difendersi

- **Controlla** sempre il **numero del mittente**
- **Non cliccare su link** dubbi
- Ricorda: **la tua banca non chiederà mai dati riservati via SMS**
- **Diffida da promesse di guadagni rapidi**

EURIZON
ASSET MANAGEMENT

Vishing: le telefonate fraudolente

Cos'è

Una tecnica di **phishing tramite chiamata telefonica**, dove il truffatore si finge un operatore di banca o assistenza tecnica.

Esempio
Una telefonata che invita a fornire i dati di accesso al conto corrente della vittima per risolvere un "problema urgente".

Come difendersi

- **Non fornire dati personali** al telefono
- **In caso di dubbio, interrompi** la chiamata e contatta l'ente ufficiale
- **Fai attenzione a toni allarmistici o pressioni**

EURIZON
ASSET MANAGEMENT

Phishing adattivo: attacco personalizzato

Cos'è

Forma evoluta di phishing, personalizzata sulla base delle abitudini o dei dati della vittima. Nel phishing adattivo elementi come il testo dell'e-mail e le immagini in essa contenute vengono modificati dinamicamente, adattandoli alla vittima colpita. L'**obiettivo** è sempre quello di convincere le vittime a condividere **informazioni sensibili.**

Esempio
E-mail che simula la schermata del proprio provider di posta, con link a una falsa pagina di login.

Come difendersi

- **Verifica URL e dominio** di provenienza
- **Non inserire mai credenziali da link ricevuti via e-mail**
- Attiva sempre **l'autenticazione a due fattori**, se disponibile

EURIZON
ASSET MANAGEMENT

Keylogger: la registrazione da tastiera

Cos'è

Con il termine keylogger, o keystroke logger, si intendono **strumenti in grado di registrare ciò che una persona digita su un dispositivo**. Possono essere **fisici**, ad esempio nascosti in un adattatore USB o **software scaricabili** dalla rete.

Esempio
Un malware scaricato da un sito fraudolento che intercetta le credenziali del proprio home banking.

Come difendersi

- **Non digitare dati sensibili su dispositivi condivisi**
- Verifica sempre la **fonte prima di scaricare**
- Usa **antivirus aggiornati** e **password robuste**
- Fate **attenzione ad eventuali manomissioni** in prossimità di porte **USB**

EURIZON
ASSET MANAGEMENT

Falso supporto tecnico: l'assistenza fasulla

Cos'è

Attraverso tecniche di social engineering, **gli aggressori contattano le vittime affermando di voler risolvere un problema tecnico fittizio o di voler eseguire un aggiornamento software** sul loro dispositivo. Chiedono così di scaricare un programma da Internet che, presumibilmente, consente l'accesso remoto al dispositivo.

Esempio
Chiamata che simula un problema su una app bancaria e invita a installare una "sicurezza" che è in realtà malware.

Come difendersi

- **Non installare software su richiesta telefonica**
- **Segnala il numero sospetto**
- **Documenta** tutto (numero, accento, richieste fatte)

EURIZON
ASSET MANAGEMENT

Deepfake: audio e video manipolati

Cos'è

Si tratta di **prodotti multimediali manipolati con intelligenza artificiale** per ingannare la vittima. Attraverso questa tecnica è possibile, infatti, modificare **video e audio** canalizzando messaggi che non corrispondono al vero: ad esempio, sovrapponendo il volto di una persona a un corpo che non è il suo e facendogli dire ciò che si vuole.

Esempio
Un video in cui una persona apparentemente affidabile propone un investimento dai facili (apparentemente) ritorni positivi.

Come difendersi

- **Verifica le fonti** dei contenuti
- **Non fidarti di richieste insolite, anche da "volti noti"**
- **Attenzione a toni allarmistici e urgenze**
- **Tieni traccia e verifica eventuali anomalie audiovisive nel contenuto multimediale**

EURIZON
ASSET MANAGEMENT

QRishing: attenzione ai QR code

Cos'è

Avete mai visto adesivi o fogli sparsi per la città con disegnato un codice QR da scansionare? **Questa tecnica si concentra sull'impossibilità per la vittima di conoscere il reale contenuto del codice QR prima della sua scansione**, ma spesso questi simboli possono nascondere minacce reali, come la richiesta di scaricare file dannosi per il dispositivo o un sito di phishing (QR + phishing = QRishing).

Esempio
Codice QR su un volantino che porta a un sito malevolo, invece che a una app ufficiale.

Come difendersi

- **Controlla che il QR non sia un adesivo sovrapposto**
- **Verifica l'URL di destinazione**
- **Usa solo app dagli store ufficiali**
- **Non scansionare QR Code senza conoscerne la fonte**

EURIZON
ASSET MANAGEMENT

False carte regalo e negozi fake: gli inganni e-shop

Cos'è

Truffe legate a e-commerce falsi o buoni regalo fittizi, spesso diffuse durante saldi o festività. **I truffatori possono agire in diversi modi, attraverso e-mail o via telefono**, ma l'**obiettivo** è sempre cercare **di ottenere informazioni riservate, come dati personali o di pagamento**.

Esempio
E-mail che promette una gift card da attivare cliccando su un link o telefonate che chiedono direttamente di pagare attraverso carte regalo bollette o tasse.

Come difendersi

- **Acquista solo su siti affidabili**
- **Diffida da offerte troppo vantaggiose**
- **Non cliccare su link** in e-mail inaspettate

EURIZON
ASSET MANAGEMENT

Truffa dell'emergenza familiare: una richiesta urgente

Cos'è

Si tratta di una truffa, perpetrata per lo più tramite SMS, in cui **i truffatori, emulando un figlio della vittima che si trova in una situazione di pericolo, chiedono di essere contattati** attraverso un contatto (cioè un numero di telefono) diverso da quello in possesso del genitore.

Esempio
Messaggio che simula un figlio in difficoltà, seguito da una richiesta di soldi.

Come difendersi

- Mantieni la **calma** e **verifica sempre**
- **Contatta direttamente la persona** che dice di essere in difficolta **tramite canali certi**
- **Non effettuare bonifici o ricariche** prima di esserne sicuri

EURIZON
ASSET MANAGEMENT

Truffe su investimenti

Cos'è

Campagne fraudolente attraverso diversi canali che promettono guadagni elevati, spesso con riferimento a criptovalute.

Esempio
SMS che invita a iscriversi a gruppi WhatsApp per "investimenti sicuri" diffondendo documenti con false informazioni.

Come difendersi

- **Diffida da promesse di guadagni rapidi**
- **Verifica** sempre **l'autenticità delle fonti**
- **Non condividere i tuoi dati** con sconosciuti

EURIZON
ASSET MANAGEMENT

Password Spraying

Cos'è

È una **tecnica usata dagli hacker per tentare l'accesso a più account usando password comuni o deboli**. Sfrutta il fatto che molti utenti riutilizzano credenziali semplici e prevedibili. Le **liste di account** vengono spesso **acquistate nel deep web o generate seguendo schemi aziendali**.

Esempio
Uso di password come "123456" o "password" su e-mail aziendali compromesse.

Come difendersi

- **Usa password robuste e uniche**
- **Attiva l'autenticazione a due fattori (MFA)** , se disponibile
- **Cambia le password predefinite al primo accesso**
- Utilizza un **password manager**

EURIZON
ASSET MANAGEMENT

Le 7 regole d'oro per la sicurezza digitale

Come abbiamo visto, **i tentativi di truffa online sono sempre più numerosi e sofisticati**.
Per questo è fondamentale **porre particolare attenzione** a ciò che ritroviamo navigando sulla rete o all'interno dei nostri smartphone, e **proteggerci** adottando alcune **semplici ma efficaci regole di sicurezza digitale:**

- **Verifica sempre il mittente** prima di cliccare o rispondere
- **Non condividere dati personali e confidenziali** tramite e-mail, SMS o telefono
- **Diffida da toni allarmistici, urgenze** sospette o **promesse** di facili guadagni
- **Controlla l'URL** prima di inserire credenziali
- **Scarica app e file solo da fonti ufficiali**
- Attiva l'**autenticazione a più fattori**, se disponibile
- **Segnala**, ove possibile, **eventuali sospetti** alle unità di supporto competenti

EURIZON
ASSET MANAGEMENT

Eurizon Capital Educazione Finanziaria

I contenuti di questo documento sono predisposti da Eurizon Capital SGR S.p.A., le informazioni e le opinioni espresse sono riferite alla data di redazione e si basano su fonti ritenute affidabili e in buona fede, tuttavia nessuna dichiarazione o garanzia è fornita dalle Società relativamente alla loro accuratezza, completezza, affidabilità e correttezza. Non vi è alcuna garanzia che i risultati o qualsiasi altro evento futuro saranno coerenti con quanto qui contenuto.

Nulla del contenuto del presente documento deve essere inteso come ricerca in materia di investimenti o comunicazione di marketing né come raccomandazione o suggerimento, rispetto ad una strategia di investimento né come sollecitazione o offerta, o consulenza in materia di investimenti, legale, fiscale o di altra natura. Qualsiasi informazione contenuta nel presente documento potrà, successivamente alla data di redazione dello stesso, essere oggetto di modifica o aggiornamento da parte di Eurizon Capital SGR S.p.A., senza alcun obbligo di comunicare tali modifiche o aggiornamenti.

Il presente documento non è rivolto a persone in giurisdizioni in cui l'offerta al pubblico di prodotti o servizi non sia autorizzata.

Eurizon Capital SGR S.p.A. e i propri dipendenti non sono responsabili né per qualsiasi eventuale danno derivante dall'affidamento fatto sulle informazioni del presente documento né per qualsiasi errore e/o omissione ivi contenuti.

I presenti contenuti non potranno essere riprodotti, ridistribuiti a terzi o pubblicati, in tutto o in parte, senza il preventivo consenso scritto da parte di Eurizon Capital SGR S.p.A..

EURIZON
ASSET MANAGEMENT

Edizione ottobre 2025

Sede Legale
Via Melchiorre Gioia, 22
20124 Milano - Italia

Eurizon Capital SGR S.p.A.
Capitale Sociale € 118.200.000,00 i.v. • Codice Fiscale e n. Iscrizione Registro Imprese di Milano 04550250015 Società partecipante al Gruppo IVA "Intesa Sanpaolo", Partita IVA 11991500015 (IT11991500015) • Iscritta all'Albo delle SGR, al n. 3 nella Sezione Gestori di OICVM e al n. 2 nella Sezione Gestori di FIA • Società soggetta all'attività di direzione e coordinamento di Intesa Sanpaolo S.p.A. ed appartenente al Gruppo Bancario Intesa Sanpaolo, iscritto all'Albo dei Gruppi Bancari Socio Unico: Intesa Sanpaolo S.p.A. • Aderente al Fondo Nazionale di Garanzia