VADEMECUM INFORMATICO PER "GIOVANI" DIGITALI

Guida pratica e strategie per un utilizzo più consapevole degli strumenti digitali

LICEO SCIENTIFICO NICCOLÒ COPERNICO
PAVIA

CHI SIAMO

Studenti del Liceo Scientifico Niccolò Copernico di Pavia, partecipanti a un progetto PON con valenza di PCTO (Percorsi per le competenze Trasversali e l’Orientamento).

OBIETTIVI

- Introdurre al mondo informatico
- Contribuire al riconoscimento di truffe online e rischi informatici
- Favorire un uso più consapevole e sicuro dei device digitali a disposizione
- Promuovere la sicurezza digitale
- Rendere gli utenti più consapevoli dell’ambiente digitale

COSA TROVERAI IN QUESTA GUIDA

PIRATERIE INFORMATICHE

Azioni in cui qualcuno non autorizzato accede, modifica, ruba o distrugge dati informatici, in violazione alle norme giuridiche vigenti.

FRODE INFORMATICA

Modifica di un sistema informatico o intervento senza permesso su dati, informazioni o programmi presenti in esso, che porta ad un danno per la persona.

PHISHING

Tipo di attacco che consiste nell'inviare email malevole scritte appositamente con lo scopo di spingere le vittime a cadere nella trappola dei cybercriminali.

SPAMMING

Lo SPAM si riferisce a messaggi indesiderati, solitamente inviati in modo massivo, per scopi pubblicitari, fraudolenti o per diffondere contenuti dannosi.

VIRUS INFORMATICI

Programma o sezione di codice introdotto nel computer senza che il proprietario ne sia a conoscenza o lo abbia autorizzato allo scopo di danneggiare file.

VIOLAZIONE DELLA PRIVACY

Raccolta, uso, condivisione o accesso non autorizzato ai dati personali, in violazione alla legge.

PAROLE UTILI

Cybercriminali: persone che usano la tecnologia e il web per fare del male agli altri. Il loro obiettivo principale è ingannare le persone per rubare soldi, password o informazioni personali come i dati della carta di credito.

Autenticazione a due fattori: sistema di sicurezza che richiede non solo una password (che è il primo fattore), ma anche una seconda verifica per accedere a un account.

Link: indirizzo digitale che ti porta da una pagina web a un'altra, o a un'altra sezione della stessa pagina.

HTTPS: connessione del tuo computer a un sito sicuro.

VPN: nasconde il tuo indirizzo IP (l'identità del tuo dispositivo su Internet), facendo sembrare che tu stia navigando da un'altra posizione o nazione e cripta i tuoi dati.

Wi-Fi aperti: rete internet gratuita e pubblica a cui puoi connetterti senza bisogno di una password.

URL: indirizzo esatto di una pagina web, un file o un'altra risorsa su Internet.

Firewall: un sistema di sicurezza che monitora e filtra tutto il traffico dati in entrata e in uscita dal tuo computer o dalla tua rete internet.

Backup: creazione di una o più copie dei dati, file e/o interi sistemi, al fine di proteggerli da eventi imprevisti che potrebbero causarli perdita o danneggiamento.

PIRATERIE INFORMATICHE

COME PROTEGGERSI

Sicurezza personale

- Password sicure e 2FA (Autenticazione a due fattori).
- Evitare link sospetti e offerte troppo allettanti.
- Non condividere dati sensibili sui social.

Strumenti di protezione

- Antivirus, Firewall e aggiornamenti regolari.
- Backup dei dati.

Navigazione sicura

- Usare HTTPS e VPN su reti pubbliche.
- Evitare Wi-Fi aperti.

ESEMPIO

L’Italian Crackdown fu un’operazione di polizia del 1994 che colpì circa 200 BBS (Bulletin Board System) in tutta Italia. L’11 e il 16 maggio 1994, la Guardia di Finanza eseguì perquisizioni e sequestri nei confronti di SysOp (amministratori) della rete FidoNet, con accuse pesanti come associazione a delinquere, pirateria informatica e violazione di sistemi. Dopo il blitz, tantissime BBS chiusero, causando il fallimento della rete Fidonet in Italia.

FRODE INFORMATICA

COME PROTEGGERSI

In aggiunta ai metodi precedentemente citati:

- Protezione dati bancari
- Controllare movimenti bancari.
- Usare carte virtuali online.

In caso di frode

- Bloccare carte/account.
- Cambiare password.
- Segnalare alla Polizia Postale.

ESEMPIO

- La Polizia ha denunciato 35 persone per una frode da 1 milione di euro contro una banca italiana. La truffa usava attacchi informatici, falsi operatori di assistenza e SMS per rubare fondi e credenziali. Grazie all'intervento della Polizia Postale, 400.000 euro sono stati recuperati.

PHISHING

COME PROTEGGERSI

- Controllare sempre il mittente
- Diffidare di richieste urgenti o minacciose
- Non cliccare su link sospetti
- Non scaricare allegati da mittenti sconosciuti
- Non fornire mai dati sensibili
- Verificare l'autenticità contattando direttamente l'ente

ESEMPIO

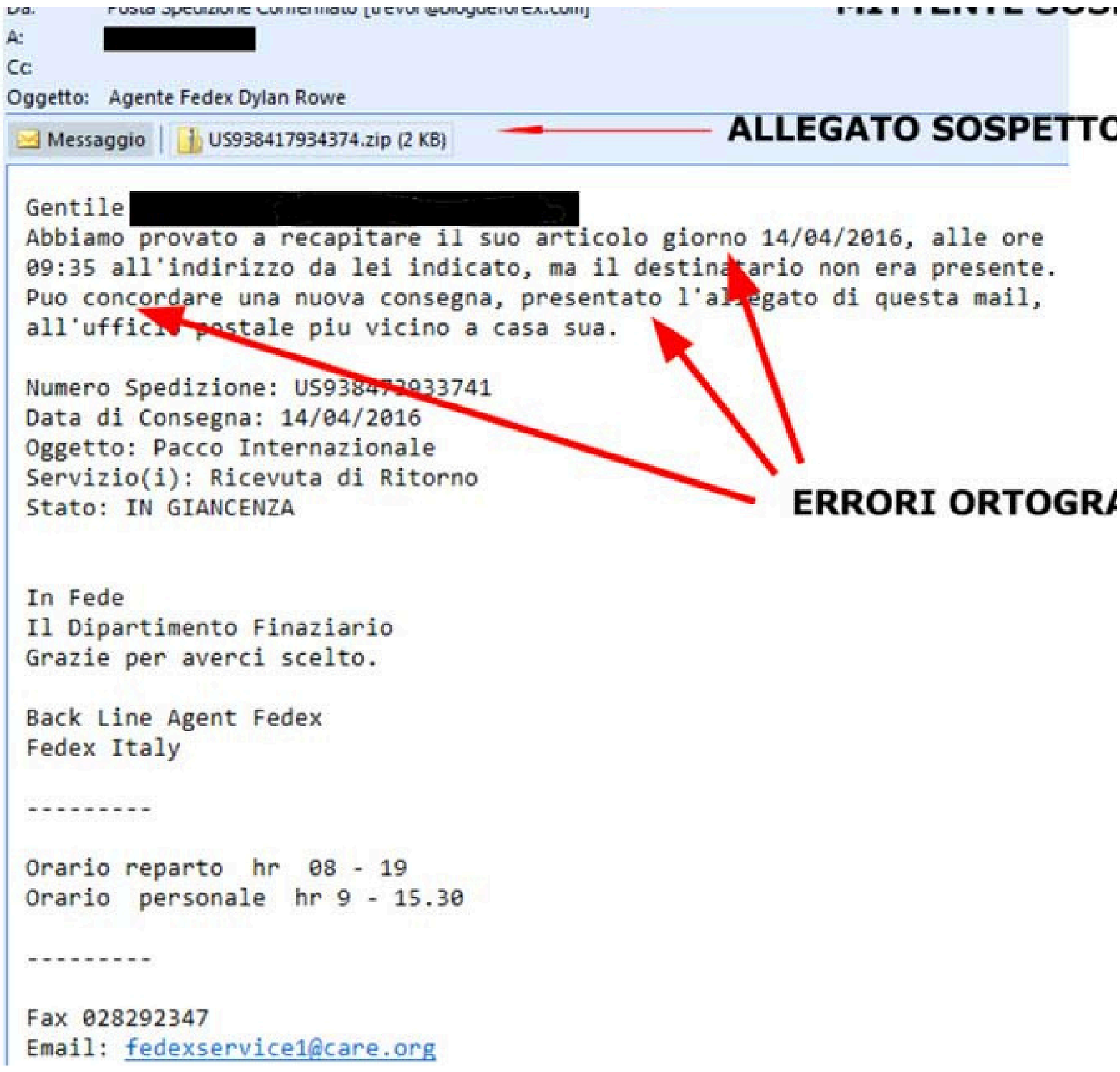
A febbraio 2025, importanti imprenditori italiani sono stati vittime di una sofisticata truffa. I truffatori hanno usato l'intelligenza artificiale per imitare la voce del Ministro Crosetto al telefono, chiedendo fondi per finti riscatti di giornalisti. Almeno un imprenditore ha trasferito un milione di euro, credendo in un rimborso dalla Banca d'Italia. Il Ministro ha denunciato l'accaduto, evidenziando l'uso dell'IA nelle nuove tecniche di frode.

SPAMMING

COME PROTEGGERSI

- Non condividere email pubblicamente
- Attenzione agli allegati sospetti
- Utilizzare un filtro antispam
- Non rispondere a SPAM
- Usare password forti e diverse per ogni account
- Controllare l'URL
- Segnalare SPAM

ESEMPIO



VIRUS INFORMATICI

COME PROTEGGERSI

- Installare un buon antivirus e aggiornarlo periodicamente
- Aggiornare regolarmente il sistema operativo e i programmi
- Diffidare di allegati e link sospetti
- Fare attenzione ai download
- Usare un firewall
- Eseguire backup regolari

ESEMPIO

LockBit è stato uno dei ransomware più attivi e pericolosi al mondo negli ultimi anni. Ha colpito aziende e organizzazioni di ogni dimensione, chiedendo ingenti riscatti per sbloccare i dati criptati. A febbraio 2024, un'operazione internazionale di polizia denominata "Cronos" ha smantellato l'infrastruttura di LockBit, sequestrando server e arrestando alcune persone collegate al gruppo.

VIOLAZIONE DELLA PRIVACY

COME PROTEGGERSI

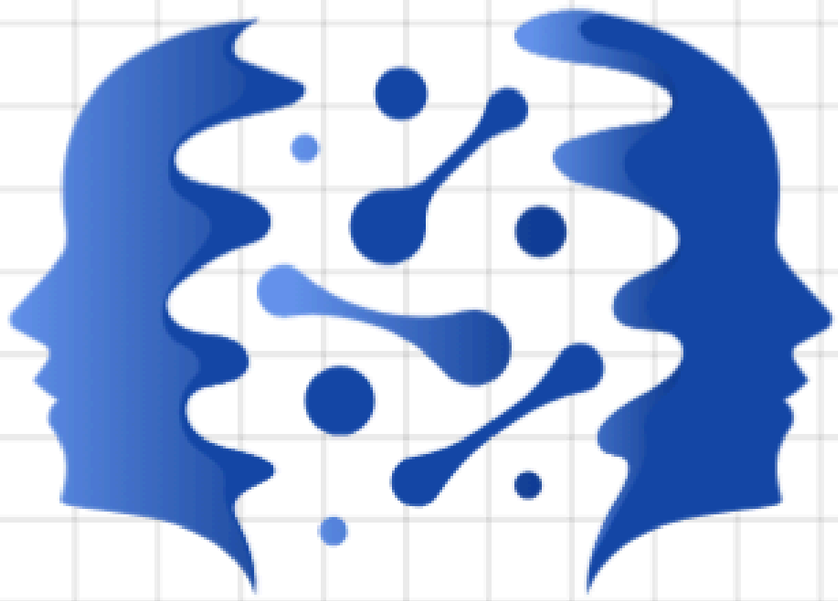
- Limitare la condivisione di dati personali
- Controllare le impostazioni privacy
- Usare password forti e uniche
- Attivare l'autenticazione a due fattori (2FA)
- Fare attenzione alle app e ai permessi concessi
- Aggiornare regolarmente software e dispositivi
- Diffidare di richieste sospette
- Usare reti Wi-Fi sicure

ESEMPIO

Durante la violazione dei dati di Facebook del 2019, i dati personali di centinaia di milioni di utenti di Facebook sono stati esposti. Le informazioni includevano numeri di telefono e altri dettagli personali, che erano stati raccolti senza le adeguate protezioni.

ESPLORA IL MONDO DIGITALE CON SERENITÀ: CON PICCOLI ACCORGIMENTI E ATTENZIONE, POTRAI GODERTI APPIENO I BENEFICI DI INTERNET, NAVIGANDO PROTETTO DALLE TRUFFE E DAI PERICOLI ONLINE.
NAVIGARE IN SICUREZZA È FACILE COME UN GIOCO: NON AVER PAURA DI CHIEDERE AIUTO, CLICCA CON CURIOSITÀ E CONTROLLA SEMPRE PRIMA DI CONDIVIDERE, PER MANTENERE LE TUE INFORMAZIONI PERSONALI AL SICURO.

BUONA NAVIGAZIONE!



COPE SECURITY AGENCY

AGGIORNA. PROTEGGI. PREVIENI.

LICEO SCIENTIFICO NICCOLÒ COPERNICO

VIA GIUSEPPE VERDI 23,25, 27100 PAVIA