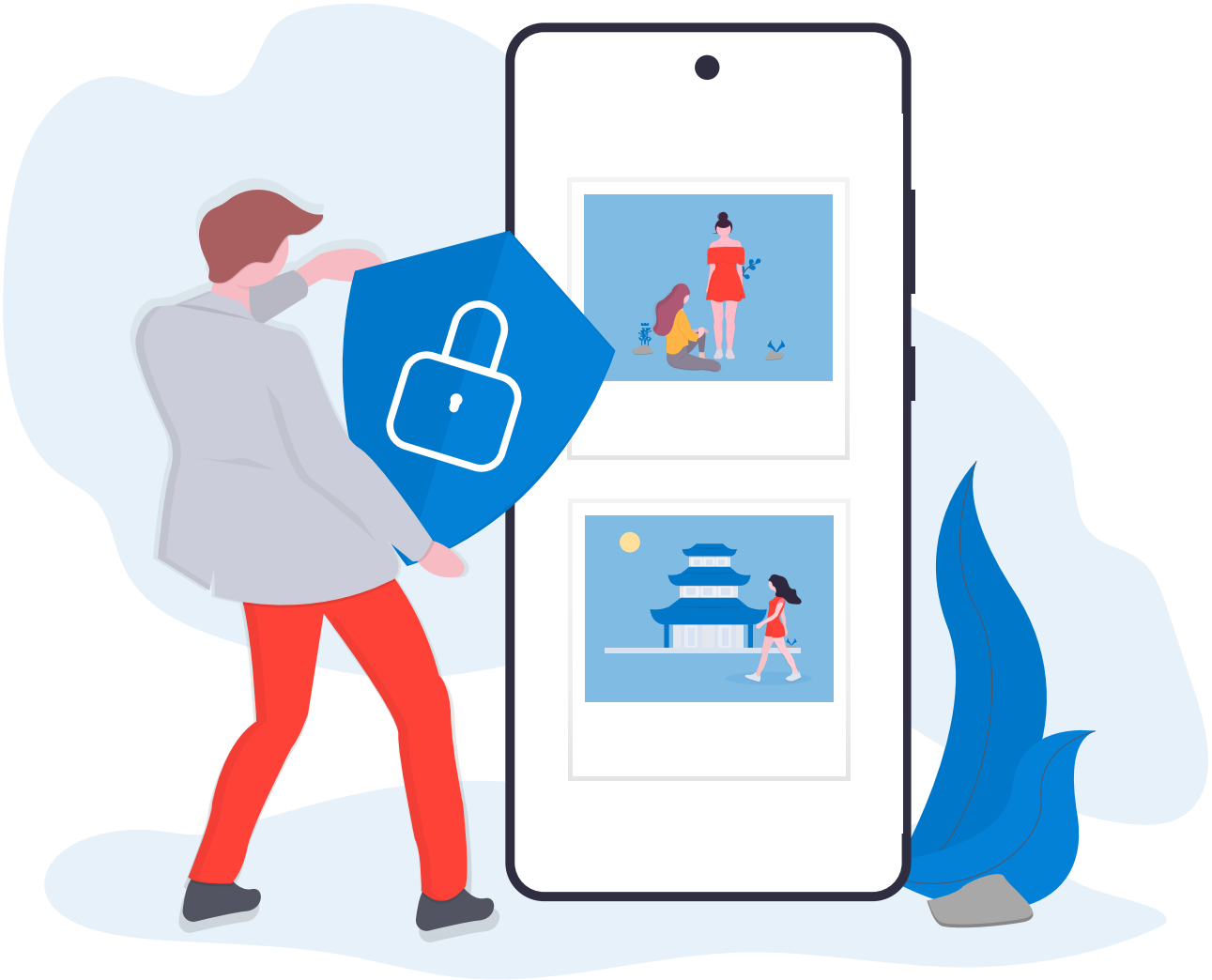
Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

Lezione 3
Sicurezza Digitale



SAMSUNG

Parola all'esperto: Riccardo Meggiato

Riccardo Meggiato è uno dei massimi esperti in sicurezza digitale, ethical hacking, investigazioni informatiche e digital forensics. Fondatore del laboratorio di informatica forense Meggiatolab, co-fondatore di una startup nel campo dei software di ricerca medica, e di una software house specializzata nello sviluppo di videogame, ha all'attivo oltre trentacinque libri best-seller; scrive su testate quali Wired, Rolling Stone, Panorama, Corriere.it e GQ; è head of content di Rolling Stone Arcade e tiene conferenze in tutta Europa, parlando di sicurezza, futuro e tecnologie software. Non si fa mai mancare un paio di ore di studio al giorno e un'ora di palestra. Lavora sette giorni su sette e dorme quattro ore a notte, e questo spiega tutto.

L'oscuro potere di un clic

Sono le 4 del mattino, state dormendo profondamente e, di punto in bianco, suona il citofono. È la Polizia, che vi comunica che siete indagati per alcuni, grossi, reati informatici, tra cui il sabotaggio di una centrale energetica e diversi furti di carte di credito. Non avete fatto nulla di tutto questo, eppure vi trovate catapultati nel bel mezzo di un incubo molto peggiore di quello che vi stava rovinando il sonno solo pochi minuti prima.

Com'è potuto succedere?

Con un clic, ma per capire meglio questa storia occorre fare un salto indietro di una settimana.

Era un venerdì pomeriggio, stavate già pregustando l'imminente weekend di fronte al vostro notebook aziendale e, tra un documento e l'altro da controllare, ecco arrivare una e-mail dal vostro boss: vi chiede di dare priorità alla compilazione del modulo in allegato e che si aspetta tutto per le 17, prima della vostra uscita, anzi fuga, dall'ufficio. Tra l'essere sollevati per l'improvviso diversivo alla solita monotonia, e l'essere un po' arrabbiati per un'aggiunta che rischia di compromettere la vostra storica puntualità alla cena del venerdì, con gli amici del Fantacalcio, decidete di aprire il modulo, un banale foglio Excel, e mettervi subito al lavoro. Ok che vi portate sempre appresso il notebook, ma "il lavoro lo si lascia in ufficio": la vostra fidanzata, su questo, è stata chiara. In realtà ci sono pochissime voci da compilare e tutto sommato vi sentite quasi in colpa per aver inveito contro il boss.

Comunque, portate a termine il lavoro e, addirittura prima delle 17, lo inviate insieme a tutto il resto.

Spegnete il notebook, lo chiudete e riponete nello zaino, e mentre state per prendere la porta dell'ufficio arriva proprio il boss a salutarvi. Ricambiate e gli dite che avete mandato tutto, modulo compreso. Lui alza il sopracciglio e vi chiede a quale modulo vi riferite e a nulla valgono le spiegazioni successive. Pare proprio che lui quella e-mail non ve l'abbia mai mandata. Poco importa, ora è tempo di weekend, fate spallucce, superate il capo e via, verso il meritato riposo.

Ora, invece, è tempo del vostro incubo reale, perché siamo tornati a quella notte e a tutto quel che sta succedendo. A proposito, ci chiedevamo: cosa è successo? In realtà, una cosa molto semplice. Ricordate il modulo? Non ve l'aveva spedito il vostro boss, ma un cyber-criminale che, al suo interno, aveva nascosto un malware, cioè un software con fini malevoli capace di trasformare il notebook in un così detto "zombie". In pratica, un computer asservito al volere del criminale. Così, mentre voi lo utilizzavate per il vostro lavoro, il criminale lo usava per le sue attività illegali, senza che ve ne poteste accorgere. E una volta beccato, in realtà, gli investigatori sono risaliti al vostro PC.

Non si tratta di fantascienza: secondo un report di WatchGuard Technologies, nel secondo trimestre del 2020 il 70% degli attacchi informatici era basato sull'utilizzo di malware "zero day", cioè malware che sfruttano i punti deboli sconosciuti di computer e smartphone. E gli esiti sono quelli che abbiamo visto in questo esempio, ma la varietà di situazioni in cui si rischia di incappare è molto più estesa. Si va dal furto dal vostro conto a quello dal conto dell'azienda per cui lavorate, dal ritrovarsi invischiati in traffici di droga in cui non c'entrate nulla, al vedersi bloccato non solo il vostro notebook ma tutta la rete aziendale, con conseguente richiesta di riscatto da parte dei criminali per sbloccare tutto. E il punto di partenza potrebbe essere proprio l'apertura di un banale allegato, oppure un clic a un link, l'inserimento di certe informazioni in alcuni moduli online, o l'utilizzo di una rete Wi-Fi poco protetta. Le attività criminali nel mondo informatico, così come le tecniche per sferrarle, sono così varie che a elencarle ci girerebbe la testa. La buona notizia, però, è che per difendersi, e limitare o evitare i danni, non serve chissà quale fatica. Giusto alcune accortezze di base. Un po' come ricordarsi di chiudere a chiave la porta di casa quando si esce, mettere il lucchetto alla bici o nascondere il portafoglio in una tasca quando si passeggia. Perché, mai come ora, la criminalità digitale deve fare più paura di quella del mondo reale. In questo booklet, per fortuna, trovate ottimi suggerimenti per difendervi.

Riccardo Meggiato

Obiettivi formativi

- Sensibilizzare sulla quantità di dati che creiamo e sul valore che questi hanno.
- Approfondire il tema della sicurezza online, sia dal punto di vista della prevenzione (impostazioni smartphone, geolocalizzazione) che dei pericoli in cui si può incorrere (frode informatica, phishing, cyber-criminalità, ransomware, ecc.).
- Introdurre il tema dei pagamenti digitali (modalità di pagamento, come avvengono, ecc.).

Indice lezione

1. Sicurezza dei device
2. Sicurezza online
3. Frode informatica
4. Pagamenti digitali
5. Attività con la classe

Capitolo 1: Sicurezza dei device

I nostri dati sono ovunque

I nostri dispositivi sono pieni di informazioni che ci riguardano, dai dati anagrafici a quelli sulla nostra vita, su ciò che ci interessa e sulle nostre abitudini. Pensate a quante cose si possono scoprire di una persona semplicemente accedendo al suo smartphone:

- Accedendo alla posta elettronica si può risalire a tutti i documenti allegati che abbiamo inviato per e-mail almeno una volta, tra i quali ci potrebbero essere Carta d'Identità e tessera sanitaria, magari anche il contratto di lavoro, quello di affitto o di acquisto della nostra casa con l'indirizzo di residenza, il libretto universitario o il registro scolastico, solo per citarne alcuni.
- Accedendo ai social network si può risalire ai nostri interessi, luoghi che frequentiamo (presenti anche sul dispositivo se abbiamo attivato la geolocalizzazione), il network di amici e le nostre abitudini.
- Il dispositivo contiene le nostre foto, video e tutti i contatti della rubrica, che potrebbero diventare a loro volta vittime di frodi.
- Le applicazioni contengono informazioni come gli estremi delle nostre carte di credito e dei sistemi di pagamento che utilizziamo online, le password e tanto altro ancora.

Sono solo alcuni esempi di tutto quello a cui è possibile risalire sull'identità e sulla vita di una persona, semplicemente accedendo al suo dispositivo personale. Proteggere questi dati è importantissimo e dobbiamo abituarci a prestare particolare attenzione a questo aspetto del mondo digitale.

Mettere in sicurezza i dispositivi

Prima di parlare di come mettere in sicurezza i dati online, è bene ricordarsi che anche i dispositivi permettono di impostare delle procedure di sicurezza che aiutano a proteggere i nostri dati, sia quelli online che quelli salvati sui dispositivi (come fotografie, video e documenti).
Per esempio, i computer consentono di bloccare lo schermo con delle password e i dispositivi mobili di bloccare lo schermo con codici numerici, password, con delle sequenze (le così dette "gesture") o con l'impronta digitale.

Vediamo nel dettaglio come proteggere i nostri dispositivi mobili come smartphone e tablet:

1. **Proteggi i tuoi dati con un blocco schermo sicuro:**
   Imposta un PIN o una password complessi e difficili da indovinare, oppure usa un blocco biometrico, come l'impronta digitale.

2. **Nascondi le informazioni più importanti:**
   Attiva Area Personale, una "cassaforte" a cui si accede con password o impronta digitale in cui puoi salvare i file più importanti e le app più sensibili, come quella della banca.

3. **Registra l'impronta digitale:**
   Con l'impronta digitale puoi accedere rapidamente a siti e app senza inserire le credenziali.

4. **Rintraccia il tuo dispositivo:**
   Se perdi un telefono o un tablet è ormai possibile individuarlo, bloccarlo o resettarlo anche da remoto. Se si tratta di dispositivi Android in cui è stato aggiunto un Account Google al dispositivo, il servizio "Trova il mio dispositivo" è automaticamente attivo. Per verificare vai su Impostazioni > Sicurezza > Trova il mio dispositivo. Per i dispositivi iOS, invece, Apple mette a disposizione la funzione "Dov'è", attivabile in questo modo: Impostazioni > Account e password > iCloud > Dov'è.

Capitolo 2: Sicurezza online

La mole di dati generata online è impressionante e tutti noi abbiamo una grandissima quantità di informazioni personali in rete. È fondamentale, quindi, tenere al sicuro queste informazioni, attraverso alcune accortezze e l'utilizzo di un sistema efficace di password.

Le password

Prestare attenzione alle password che si utilizzano è importantissimo per proteggere i propri dati personali. Ecco alcune regole generali:

- Mai utilizzare la stessa password per più di un sito, meglio inventarsene una nuova per ogni sito e servizio a cui ci si iscrive.
- Utilizzare password complesse, di almeno 12 caratteri, contenenti lettere, numeri, maiuscole e, dove consentito, caratteri speciali, difficili da crackare.
- Sostituire periodicamente le password: alcune aziende, per esempio, le fanno cambiare a tutti i dipendenti ogni 75-90 giorni. In altre aziende ancora, gli IT manager provvedono a programmare cambi periodici automatici.
- Utilizzare un tool per gestire le password (password manager) e non rischiare di dimenticarle.
- Rafforzare la sicurezza della password, utilizzando le domande di sicurezza o la cosiddetta verifica in due passaggi, che include un codice numerico da inviare sul telefono per rendere più difficoltoso l'accesso all'account da un nuovo device.
- È anche buona norma ricordarsi di effettuare il log out dai siti che richiedono l'inserimento delle proprie credenziali, se si utilizza un dispositivo condiviso o che può essere raggiunto da altri.
- Non condividere mai e per nessuna ragione le proprie password: una persona fidata oggi, potrebbe diventare inaffidabile domani. E nel frattempo potremmo esserci scordati di quali password le abbiamo consegnato.

Antivirus

Per evitare di contrarre malware navigando su Internet, oppure aprendo e-mail che sembrano innocue, occorre avere sempre un antivirus aggiornato e in funzione sui propri device. Evitate, invece, di installarne due come consigliato anche da alcuni esperti: rischierebbero di andare in conflitto tra loro, perdendo entrambi di efficacia. Anche aggiornare i propri software e sistemi aiuta a mantenere i propri dati personali al sicuro.

La posta elettronica

La casella di posta elettronica è uno degli strumenti più utilizzati ogni giorno e uno degli aggregatori di dati personali più importanti. Nei nostri scambi di e-mail abbiamo dati bancari, documenti personali, estratti conto, risultati di esami e tutto ciò che riguarda la nostra vita. È indispensabile, quindi, porre in sicurezza le nostre caselle ed evitare di mettere in pericolo le informazioni che ci riguardano.

La prima cosa da fare per non correre rischi è evitare di aprire allegati sospetti o di cliccare su link contenuti nel corpo del messaggio, soprattutto se questo proviene da un mittente non attendibile.

In ogni caso, quando non si è sicuri dell'identità del mittente, meglio verificarla e, se si tratta di un nostro conoscente, contattarlo in altro modo per assicurarsi che il messaggio provenga dal suo indirizzo.

I profili social

Anche mantenere un discreto livello di privacy sui propri profili social è di certo un buon metodo per proteggere i propri dati. È importante selezionare bene i contatti, prestare attenzione a chi si aggiunge al proprio network, controllare e restringere la privacy di alcuni contenuti pubblicati, limitandone l'accesso ad amici o gruppi, e non pubblicare mai informazioni personali come numero di telefono o indirizzo e-mail.

Facebook e Instagram, per esempio, offrono una serie di opzioni personalizzabili per modificare le impostazioni sulla privacy di ciascun profilo: prendersi cura di questo aspetto è molto importante. Inoltre, mantenere privati i contenuti del proprio profilo scoraggia i cyber-criminali dal rubare la nostra identità e le nostre foto.

Capitolo 3: Frode informatica

Frodi informatiche

Oltre a proteggere i nostri dispositivi, dobbiamo fare attenzione anche a quando navighiamo online: in rete, infatti, si può cadere vittime di malware, truffe e messaggi ingannevoli ed è quindi importante conoscere le principali tecniche che i malintenzionati usano per attaccare online.

Per aggirare antivirus e sistemi di sicurezza, sono state sviluppate delle tecniche per lo studio e la manipolazione dei comportamenti delle persone con lo scopo di raccogliere informazioni confidenziali. L'insieme di queste tecniche prende il nome di **"Ingegneria sociale"**.

I principali metodi che rientrano nell'ingegneria sociale sono:

- **Phishing:** consiste nell'ingannare la vittima a condividere i propri dati tramite l'invio di messaggi o e-mail ingannevoli
- **Vishing:** è la versione telefonica del phishing
- **Pretexting:** consiste nel fingere di essere entità considerate affidabili (banca, posta, pubbliche amministrazioni...) sfruttando dei dati sull'utente che già si conoscono (data di nascita, indirizzo di residenza...) per spingerlo a divulgare informazioni confidenziali
- **Baiting:** consiste nell'utilizzare un'esca (come una chiavetta USB, contenente un malware, che viene lasciata incustodita) per stimolare la curiosità della vittima e indurla a raccogliere l'oggetto, che una volta inserito in un PC diventerà un punto di accesso per i sistemi aziendali.

Queste tecniche sono particolarmente insidiose perché cercano di ingannarci, cercando di indurci a fidarci di chi ci sta contattando. Il phishing, in particolare, esiste ormai da molti anni ma rimane uno degli attacchi più efficaci. Vediamolo nel dettaglio.

Phishing

Parliamo di phishing (da «to fish», «pescare», perché la vittima viene «presa all'amo» dal truffatore) quando qualcuno cerca di rubarci l'identità o i dati per accedere ai nostri conti bancari, carta di credito o per altre operazioni criminali, e generalmente lo fa spacciandosi per qualcun altro. Un tipico messaggio di phishing arriva via e-mail e sembra provenire da una banca o da un'organizzazione conosciuta che, solitamente, segnala un grave problema tecnico da risolvere al più presto. Il messaggio generalmente chiederà di cliccare su un link, che conduce a un modulo dove inserire i nostri dati bancari o personali, induce a installare un malware, o addirittura a rispondere direttamente coi nostri dati, password o codici di accesso.

Qualunque messaggio che richieda l'inserimento di dati personali, password o codici di accesso, pena la cancellazione di un account o il blocco di un conto, va immediatamente segnalato e cestinato.

Ricordiamoci che le banche o le compagnie telefoniche non inviano mai una richiesta sollecita di inviare i nostri dati sensibili via posta elettronica.

I messaggi provenienti da mittenti sconosciuti e contenenti link sospetti e pulsanti che invitano a cliccare su dei link per compiere delle azioni, come "Verifica subito", "Vai al sito" ecc.; e anche gravi errori ortografici, sono probabilmente tentativi di phishing che vanno segnalati.

Inoltre, i messaggi di phishing contengono spesso errori grammaticali, a volte i loghi delle organizzazioni sono riprodotti male e invitano sempre a cliccare per risolvere il problema immediatamente, pena la chiusura o disattivazione del nostro account. Non è difficile riconoscerli, basta fare attenzione.

Come riconoscere i messaggi ingannevoli?

Le immagini di seguito contengono esempi di phishing via SMS e via e-mail:

Numero di telefono sconosciuto.

Il messaggio arriva da un numero di telefono che non abbiamo salvato in rubrica. Bisogna fare sempre molta attenzione ai messaggi che riceviamo da numeri sconosciuti.

Link sconosciuto.

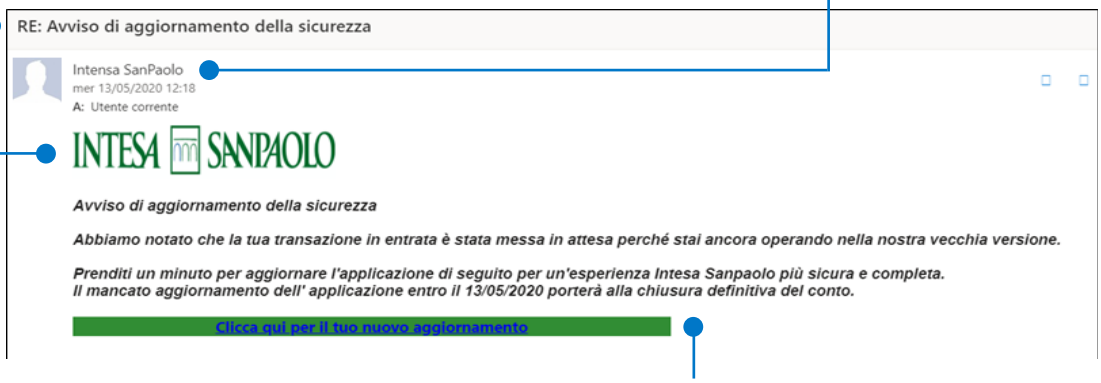
Il link non porta a nessun sito di banche o altre istituzioni note. Non bisogna mai cliccare su link sconosciuti perché potrebbero portare a pagine dannose.

Contenuto generico.

Nel messaggio non viene specificato chi è il mittente, né di che tipo di conto si tratta. Inoltre, non vengono dati dettagli sul motivo della presunta sospensione del conto.

Oggetto sospetto.
In questo caso, l'oggetto dell'e-mail è strutturato come risposta a un messaggio ("RE:"). Se non abbiamo inviato nessuna e-mail a questo mittente, il messaggio è falso.

Mittente sconosciuto.
Il mittente in questo caso appare come "Intensa SanPaolo", che non è il nome corretto della banca.



Logo non corretto.
Il logo non rispetta le proporzioni di quello reale della banca.

Canale non ufficiale.
L'e-mail suggerisce di cliccare sul link per aggiornare l'app: gli aggiornamenti avvengono sempre e solo attraverso gli store ufficiali, per cui questo link non è affidabile.

Per riconoscere le e-mail maligne, ci sono alcuni suggerimenti da ricordare:

1. **Verificare il mittente:** prima di aprire il messaggio, dobbiamo controllare da chi arriva e fare molta attenzione in caso di mittenti sconosciuti.
2. **Leggere l'oggetto:** se l'oggetto della e-mail non è chiaro, è molto generico, o è scritto in inglese, potrebbe trattarsi di una e-mail maligna.
3. **Non dare mai dati personali:** a volte l'indirizzo può sembrare affidabile, ma se vengono richiesti dei dati (password, numeri di carta di credito, ecc.), non bisogna mai fornirli. Nessuna banca o ente ufficiale raccoglie i dati via e-mail.
4. **Non scaricare gli allegati:** in caso di mittente sconosciuto, bisogna evitare di scaricare gli allegati. Se invece conosciamo il mittente, possiamo verificare con lui/lei che l'e-mail sia vera e l'allegato non pericoloso.
5. **Non aprire i link:** un link è un rimando ad un sito Internet e potrebbe portare a pagine web maligne. Prima di aprirli, è sempre meglio verificare con il mittente, se conosciuto, o non aprirli se il mittente è sconosciuto.
6. **"Capire" le e-mail:** una e-mail andrebbe sempre letta con attenzione. Richieste strane o non coerenti con un mittente che di solito adotta un altro stile o parla di altri contenuti potrebbero essere indicative di una e-mail truffaldina.
7. **Il trucco del reply:** le e-mail malevole, in genere, sono fatte per convincerci a cliccare su un link o scaricare un allegato, ma non per ricevere le nostre risposte. Così, se facciamo un reply a una e-mail sospetta, e riceviamo un errore di invio o ricezione perché l'indirizzo del destinatario sembra essere inesistente, potremmo avere la conferma di essere di fronte a una trappola digitale.

In generale, banche, poste, pubbliche amministrazioni ed entità simili comunicano sempre attraverso i loro canali ufficiali e non chiedono mai di inserire o confermare dati personali, password o numeri di carta di credito via e-mail o SMS. In caso di dubbi, è meglio contattare il presunto mittente del messaggio attraverso i canali ufficiali e verificare che la richiesta sia reale.

Le truffe si possono anche basare su finte vincite, con e-mail che parlano di premi o somme di denaro: queste e-mail vanno sempre ignorate e cancellate.

Capitolo 4: Pagamenti digitali

Per evitare di cadere vittime dei tentativi di frode appena visti è bene imparare come funzionano le transazioni e i pagamenti digitali, in modo da prendere confidenza coi vari metodi e riconoscere subito eventuali tentativi di frode.

I metodi di pagamento

Sono molti i metodi di pagamento riconosciuti e accettati in Italia, alcuni più tradizionali e in uso ormai da secoli, come il contante, e altri di più recente introduzione, come le carte di credito: queste ultime rientrano nella categoria dei cosiddetti "pagamenti digitali".

Per "pagamenti digitali" si intendono tutti quei pagamenti effettuati con strumenti di pagamento elettronici, come appunto le carte di credito. I pagamenti digitali offrono molti vantaggi rispetto alle forme di pagamento tradizionali: possono più facilmente essere tracciati, per esempio per motivi fiscali, possono essere bloccati in caso di furto e danno la possibilità di ottenere più facilmente rimborsi in caso di reso del prodotto o di truffe. Usando pagamenti digitali, inoltre, non dovremo preoccuparci di cambiare la valuta se andiamo all'estero, poiché il cambio è gestito automaticamente dal circuito di pagamento.

I "circuiti" sono società che gestiscono le richieste e le autorizzazioni di pagamento che avvengono in modalità elettronica, mettendo in comunicazione il POS (cioè il lettore delle carte di pagamento, presente ormai in tutti i negozi) con la banca o l'istituto che ha emesso la carta. Esempi di circuiti di pagamento tra i più diffusi sono Visa e MasterCard.

Tra le modalità di pagamento digitale rientrano:

- le carte di credito, debito o prepagate, che vengono utilizzate con i tradizionali POS oppure per gli acquisti online
- i pagamenti effettuati con lo smartphone, attraverso siti web, app e mobile wallet

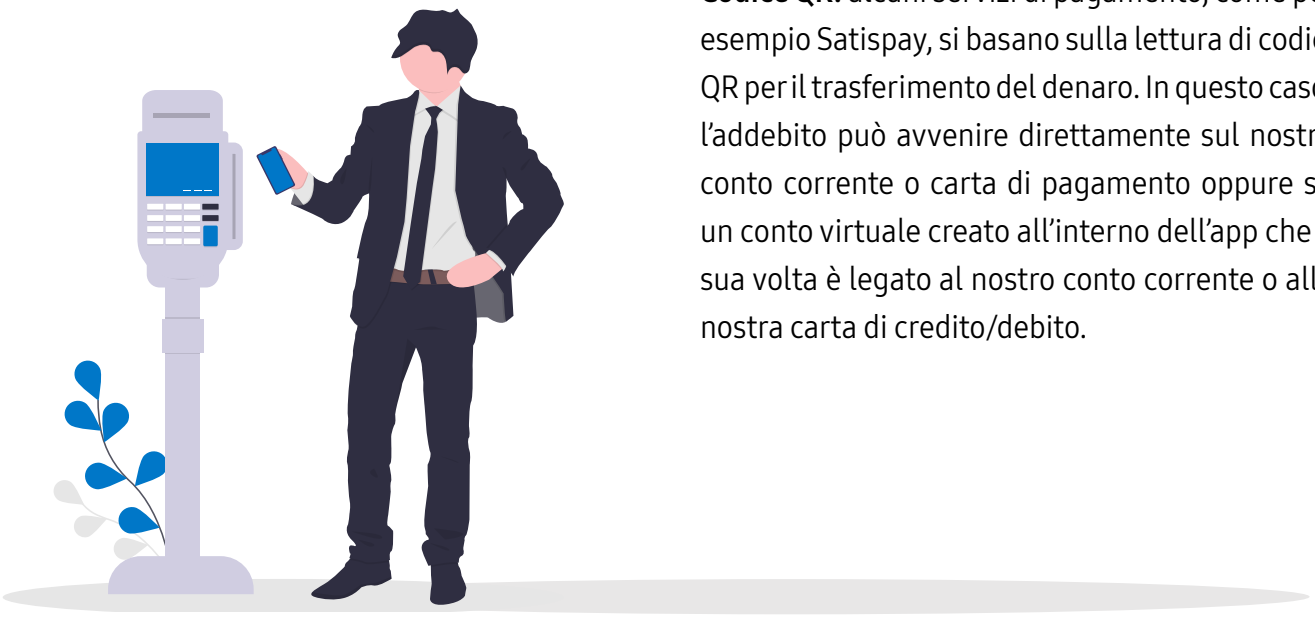
I *mobile wallet (o e-wallet)* sono portafogli digitali che vengono creati e gestiti sullo smartphone e possono contenere, oltre alle carte di pagamento, anche carte fedeltà, carte di imbarco, biglietti dei trasporti pubblici e molto altro.

Pagare con lo smartphone

Ci sono diverse modalità di pagamento con lo smartphone, che si raggruppano in:

- **Mobile Remote Payment:** sono tutti quei pagamenti digitali effettuati tramite lo smartphone da remoto, cioè non presso un punto vendita. Rientrano in questa categoria le transazioni eseguite attraverso app per lo shopping online, per i pagamenti di bollettini, ricariche telefoniche o biglietti dei trasporti pubblici.

- **Mobile Proximity Payment:** sono i pagamenti che avvengono presso un punto vendita e che sono effettuati con l'uso dello smartphone. Questa tipologia è sempre più diffusa come sostituto dei pagamenti tradizionali in contanti o con carte di pagamento fisiche. È una categoria molto vasta, che include modalità di pagamento basate su diverse tecnologie:



- **NFC (Near-Field Communication):** è una tecnologia che consente lo scambio immediato e sicuro di dati da un dispositivo a un altro (nel caso dei pagamenti, dallo smartphone al POS) a una distanza molto ravvicinata. Su questa tecnologia si basano le app di pagamento più diffuse, come Samsung Pay, Apple Pay o Google Pay: queste app consentono di creare una "versione digitale" della nostra carta di pagamento sullo smartphone. Aprendo l'app, e avvicinando il telefono al POS, potremo concludere il pagamento proprio come si fa con le carte fisiche. Per verificare la nostra identità, queste app utilizzano un PIN oppure un metodo di riconoscimento biometrico, come le impronte digitali o il riconoscimento del viso. Le app di questo tipo addebitano il costo sulla carta di pagamento che abbiamo scelto di digitalizzare.

- **Codice QR:** alcuni servizi di pagamento, come per esempio Satispay, si basano sulla lettura di codici QR per il trasferimento del denaro. In questo caso, l'addebito può avvenire direttamente sul nostro conto corrente o carta di pagamento oppure su un conto virtuale creato all'interno dell'app che a sua volta è legato al nostro conto corrente o alla nostra carta di credito/debito.

- **Peer-to-peer Payment:** spesso abbreviato in P2P, si tratta dello scambio di denaro tra privati. Ci sono molte soluzioni che consentono di trasferire soldi ai nostri amici in modalità digitale, gratuitamente e in tempo reale. Alcune di queste app si appoggiano direttamente al conto corrente, mentre altre consentono di creare un conto virtuale prepagato che possiamo ricaricare quando necessario, ma hanno tutte in comune un'estrema semplicità di utilizzo: ci basterà infatti avere il numero di telefono o l'indirizzo e-mail della persona a cui vogliamo inviare il denaro per completare il trasferimento. Alcune delle app più diffuse che offrono questa funzionalità sono PayPal, Circle, Jiffy e Satispay e sono molto utili, per esempio, per dividere un conto al ristorante o per raccogliere quote per un regalo di gruppo.

Sicurezza nei pagamenti digitali

Esiste una normativa europea che regola i pagamenti digitali e garantisce che tutte le app e le piattaforme che offrono servizi di pagamento seguano dei criteri molto rigidi di sicurezza. Questa normativa, entrata in vigore nel Gennaio 2018, si chiama Payment Services Directive 2 (Direttiva dei Sistemi di Pagamento 2) o PSD2 e sostituisce la precedente PSD del 2007.

La principale novità introdotta nell'ambito della sicurezza riguarda l'obbligo di adottare nuovi e più sicuri sistemi di autenticazione basati sulla Strong Customer Authentication (Autenticazione forte del cliente o SCA). Questo sistema serve a identificarci in modo univoco quando utilizziamo i pagamenti digitali, per evitare che altre persone possano utilizzarli a nostro nome o a nostra insaputa.
In caso di transazioni non autorizzate, poi, è possibile chiedere un rimborso al circuito di pagamento che, se verificherà un uso illecito della nostra carta, ci potrà restituire la somma addebitata. Possiamo facilmente tenere sotto controllo le transazioni abilitando i messaggi di notifica: questo servizio ci invia un SMS, un'e-mail oppure una notifica via app ogni volta che utilizziamo i nostri mezzi di pagamento digitali, permettendoci di avere sempre le spese sotto controllo ed essere informati tempestivamente in caso di spese non autorizzate. Le carte, inoltre, possono facilmente essere bloccate in qualunque momento, telefonando alla nostra banca.

Se dovessimo invece perdere lo smartphone, o ci venisse rubato, è possibile bloccarlo e cancellare da remoto i nostri dati grazie ai servizi di localizzazione dei dispositivi (come Find my mobile o Find my iPhone): in questo modo, nessun altro potrà usare i nostri strumenti di pagamento digitale dal nostro smartphone.
Queste operazioni non sono invece possibili per i contanti, che non possono in alcun modo essere bloccati o rintracciati.

Dove si può pagare con gli strumenti digitali?

È possibile utilizzare le carte di pagamento fisiche presso tutte le attività commerciali che sono dotate di POS, cioè lo strumento necessario per leggere le carte. Nel caso in cui il POS sia abilitato al pagamento *contactless* (cioè appoggiando la carta al lettore) è anche possibile pagare attraverso le app basate su tecnologia NFC che digitalizzano le nostre carte di pagamento (Samsung Pay, Apple Pay, Google Pay, ecc.).

Già dal 2014, in tutta Italia, è obbligatorio per negozi, ristoranti, hotel e tutte le attività commerciali dotarsi di POS, anche se non tutti si sono adeguati. I POS, comunque, soprattutto quelli contactless, sono ormai molto diffusi e questo ci permette di utilizzare i nostri strumenti di pagamento digitali quasi ovunque.

Accettare pagamenti non basati sulle carte di credito o debito (per esempio Satispay) è invece una scelta dell'esercente, ma molti stanno adeguando anche a questi metodi.
In alcuni casi è addirittura obbligatorio usare pagamenti digitali: per pagamenti superiori a 2.000€, infatti, dal 1 luglio 2020 è vietato utilizzare i contanti.

ATTIVITÀ CON LA CLASSE

Attività 1 - Oggetti dimenticati

- Materiale necessario: connessione a Internet, possibilità di proiettare
- Obiettivo: rendere gli studenti consapevoli dell'importanza di tutelare i propri dati

Vengono proiettate le immagini di oggetti e luoghi che trent'anni fa erano utilizzati per le stesse azioni di oggi (un walkman, un telefono a cornetta, una cartina geografica, una console Nintendo, una macchina Polaroid, una cabina telefonica, una macchina da scrivere, una cinepresa, un videoregistratore, uno stereo portatile...).
Gli oggetti sono disponibili su www.conservethesound.de

- Viene chiesto agli studenti di individuare gli oggetti che trent'anni fa permettevano di compiere determinate azioni: per esempio, con quale di questi oggetti si ascoltava la musica? Come ci si orientava per strada? Con cosa si giocava? Probabilmente non riconosceranno gran parte degli oggetti. L'attività permette di spiegare che fino a non molto tempo fa molte azioni erano delegate a oggetti singoli analogici, mentre oggi vengono racchiuse tutte in formato digitale all'interno di un unico oggetto, il telefonino.
- Ma cosa sarebbe successo trent'anni fa se avessi perso il walkman, il Nintendo o la cartina geografica? Si perdeva solamente un oggetto, mentre oggi si perde qualcosa di molto più prezioso: i nostri dati. Accade per esempio se rubano il mio account Spotify o Netflix, o quello della Playstation. Oppure posso condividere informazioni sui miei spostamenti mentre uso Google Maps, se è impostata la geolocalizzazione.
- Un account è l'insieme di dati identificativi di un utente che gli/le consentono l'accesso a un servizio telematico. Viene chiesto agli studenti quali dati andrebbero persi se venissero rubati gli account digitali di Netflix, Spotify, o altre applicazioni che permettono di compiere le azioni descritte nel primo esercizio. Si scoprirà che potrebbero essere messi a rischio la casella email, il profilo Facebook con contatti e informazioni personali, fino ai dati di pagamento della carta di credito associata all'account. Anche il furto di un account Playstation potrebbe permettere al ladro di accedere al profilo personale dell'utente per poterlo gestire a proprio piacimento, effettuando il download di giochi con la carta di credito a esso collegata.
- Poiché i dispositivi tecnologici di oggi non sono semplici oggetti ma racchiudono in un certo senso la nostra vita, è importante proteggere i propri dati e prendere provvedimenti per impedire l'accesso di utenti indesiderati. Una buona pratica è uscire dal proprio account sui tutti i dispositivi che non vengono solitamente utilizzati. Il sistema del Centro Assistenza invia solitamente un'email ogni volta che rileva un accesso sospetto da un nuovo dispositivo: se non riconosci l'accesso, cambia subito la password.

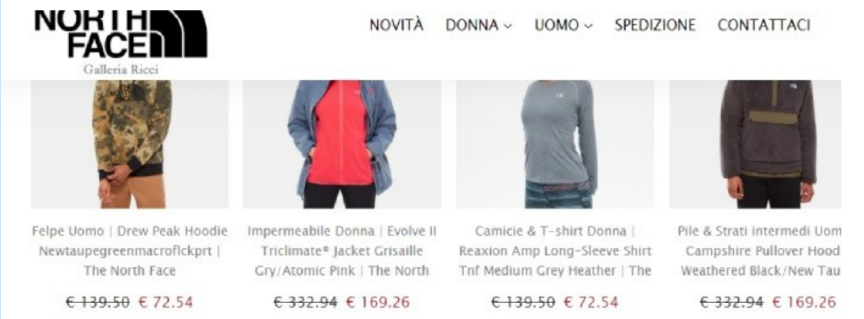
ATTIVITÀ CON LA CLASSE

Attività 2 - Non ci casco!

- Materiale necessario: possibilità di proiettare
- Obiettivo: fornire agli studenti strumenti su come riconoscere truffe online

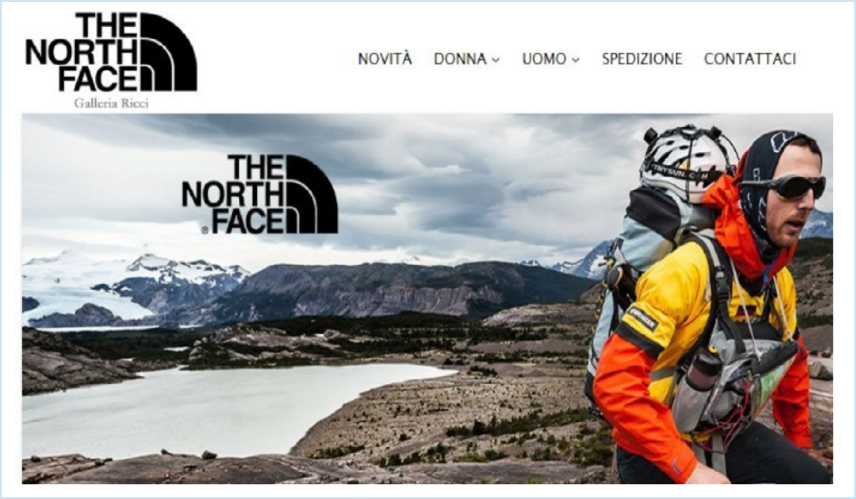
Esistono purtroppo molte notizie riguardanti falsi negozi online, che rubano i soldi dei clienti e spariscono nel nulla dopo averli attirati con recensioni false e annunci pubblicitari offrendo prezzi stracciati (anche del 60% rispetto al prezzo originale di listino). Di solito il sito truffa è costruito bene ed è spesso molto simile a quello originale. Per questo è facile caderci!

Ma come si fa a capire se un sito è una truffa?
L'insegnante proietta un esempio di sito truffa www.galleriaricci.it (senza svelare che si tratta di un fake) chiedendo agli studenti di osservare se c'è qualcosa che non quadra e se acquisterebbero o meno dal sito.



Il sito presenta capi d'abbigliamento costosi a prezzi veramente bassi. Inoltre il protocollo HTTPS nella URL è assente. Ma non finisce qui...ci sono altre differenze!

Consiglio n°1: controlla il dominio e diffida dei siti che propongono prodotti costosi a prezzi stracciatissimi

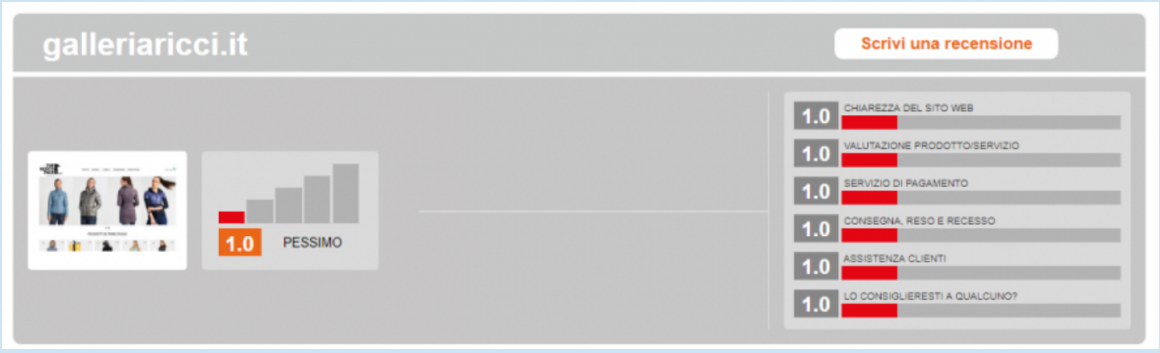


Il negozio online fasullo presenta il nome di un brand insieme al nome di una galleria d'arte moderna... ma vende capi d'abbigliamento!

Consiglio n°2: verifica nome del sito e corrispondenza dei prodotti

ATTIVITÀ CON LA CLASSE

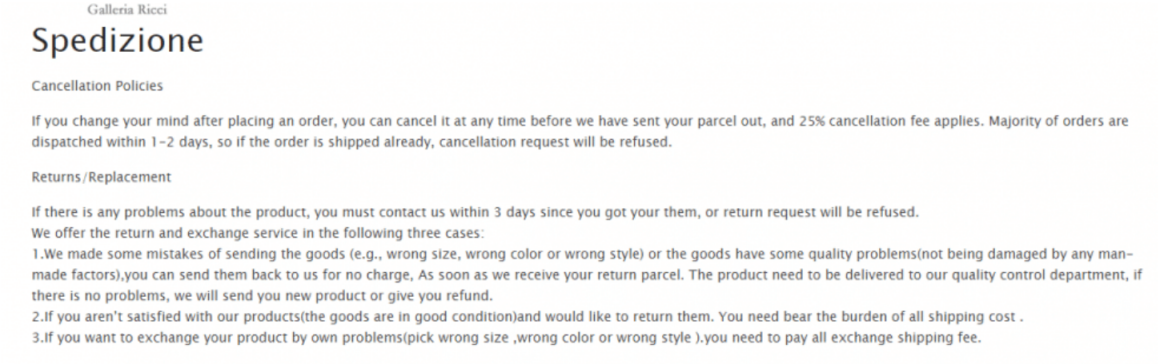
Osserviamo adesso la seguente tabella: cosa notate?



Consiglio n° 3: leggi sempre le recensioni sul negozio
Questa è la cosa più semplice: spesso i siti truffa sono pressoché sconosciuti (se non fosse per gli annunci online), quindi mancano le recensioni oppure sono poche e pessime.

Consiglio n° 4: verifica sempre che sul sito sia presente una partita IVA reale
I siti truffa scrivono spesso sul sito una partita IVA inventata o appartenente ad un'altra azienda. Ma come scoprirlo? Basta verificarlo sul sito ufficiale dell'**Agenzia delle Entrate:**
https://telematici.agenziaentrate.gov.it/VerificaPIVA/Scegli.do?parameter=verificaPiva

Per l'ultimo consiglio, leggiamo cosa ci dice la pagina dedicata alle policy di spedizione...


Galleria Ricci

Spedizione

Cancellation Policies

If you change your mind after placing an order, you can cancel it at any time before we have sent your parcel out, and 25% cancellation fee applies. Majority of orders are dispatched within 1~2 days, so if the order is shipped already, cancellation request will be refused.

Returns/Replacement

If there is any problems about the product, you must contact us within 3 days since you got your them, or return request will be refused.
We offer the return and exchange service in the following three cases:
1.We made some mistakes of sending the goods (e.g., wrong size, wrong color or wrong style) or the goods have some quality problems(not being damaged by any man-made factors),you can send them back to us for no charge, As soon as we receive your return parcel. The product need to be delivered to our quality control department, if there is no problems, we will send you new product or give you refund.
2.If you aren't satisfied with our products(the goods are in good condition)and would like to return them. You need bear the burden of all shipping cost .
3.If you want to exchange your product by own problems(pick wrong size ,wrong color or wrong style).you need to pay all exchange shipping fee.

Il titolo è in italiano e la descrizione in inglese!

Consiglio n° 5: verifica che la grammatica dei contenuti sia corretta
In generale controllare se i testi presentano errori grammaticali o se sono tradotti solo in parte.