PER I CITTADINI E I RAGAZZI























INTERNET: RISCHI E MINACCE

INDICE



ARGOMENTO	NUMERO SLIDE
Uso sicuro del telefono	3
Blocco carte di credito	4
Utilizzo della carta sulla rete	5
eCommerce	6
Hacking	7
Money Muling	8
Phishing	9
Spamming	10
Pedofilia online	11
Cyber Hygiene	12
Social network	13
Cyberstalking	14









https://www.commissariatodips.it/consigli/per-i-cittadini-e-i-ragazzi/internet-qualche-precauzione/index.html



Utilizzare il telefono in modo sicuro

Come utilizzare il telefono in modo sicuro?

Non richiamare col telefonino numeri sconosciuti

Non pubblicare foto o filmati fatti con il telefonino in community o chat telefoniche che siano aperte a tutti

Modifica le tue impostazioni tutelando sempre la tua privacy.

Custodisci il tuo numero di telefonino e dallo solo alle persone di cui ti fidi.

NON fornire informazioni personali .a chi conosci nelle chat telefoniche poiché non hai modo di verificare la sua buona fede.

Non rispondere a messaggi di sconosciuti, sono truffe.

Usa le immagini che raccogli nel **rispetto** degli altri, **evitando** così di commettere illeciti anche involontari.

Informa i tuoi genitori se le telefonate si fanno frequenti, se arrivano in orari strani o se a chiamarti sono adulti/e sconosciuti.



Usa i social e le app con attenzione

TI HANNO RUBATO LA CARTA DI CREDITO ?
COSA DEVI FARE ?

SE TI HANNO RUBATO RUBATO LA CARTA DI CREDITO È NECESSARIO BLOCCARLA IMMEDIATAMENTE

CONSIGLI:

BISOGNA CHIAMARE IL NUMERO (GRATUITO) DELLA SOCIETÀ EMITTENTE DELLA TUA CARTA DI CREDITO, IL PIN VERRÀ BLOCCATO AUTOMATICAMENTE

- OSSERVARE LE CONDIZIONI DELLO SPORTELLO
- CONTROLLARE CHE NON CI SIA UNA MICROTELECAMERA.
- CONTROLLARE CHE LA BOCCA DELLA FESSURA NON SI STACCHI O SI MUOVA
- VERIFICARE CHE ANCHE LA TASTIERA SIA BEN FISSA
- DIGITARE IL PROPRIO PIN NASCONDENDOLO CON IL PALMO DELLA MANO
- SE SI HANNO DUBBI, ALLONTANARSI DALL' ATM E CONTATTARE LE AUTORITA'



DI SOLITO I MALFATTORI SONO APPOSTATI PER CONTROLLARE LA SITUAZIONE E CON UN COMPUTER CON TECNOLOGIA SENZA FILI RICEVONO INFO E IMMAGINI DALLA TELECAMERA.

L' UTILIZZO DELLA CARTA SULLA RETE INTERNET

COME USARE LA CARTA DI CREDITO ?

Evitare di fornire troppe informazioni personali o relative al proprio conto corrente all'interno di un sito.

N.B. le transazioni per andare a buon fine necessitano solamente del numero della carta di credito e relativa scadenza.

Verificare con attenzione gli estratti conto segnalando immediatamente alla società emittente ogni transazione sconosciuta.



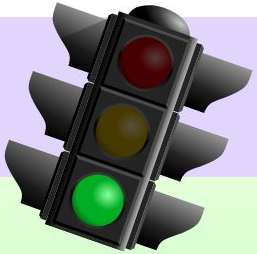
Fare uso delle varie soluzioni di home banking, messe a disposizione dalle banche, per controllare quasi in tempo reale il proprio estratto conto, così da bloccare tempestivamente la carta qualora si disconoscessero delle spese addebitate.

E-COMMERCE



L'insieme delle attività di vendita e acquisto di prodotti effettuato tramite Internet





- **VERIFICARE** l' esistenza di segnalazioni riguardanti il venditore
- **UTILIZZARE** carte prepagate che possono essere ricaricate in anticipo con la quantità di denaro da utilizzare, per prevenire il furto di tutto il denaro del conto bancario



- **UTILIZZARE** la carta di credito in sicurezza
- NON **DIFFONDERE** troppe informazioni personali
- NON **NAVIGARE** in falsi siti , dove spesso vengono pubblicizzati oggetti di marche costose a un prezzo molto basso;
- **CAMBIARE** la password FREQUENTEMENTE,
- **DIFFIDARE** di prodotti, SOPRATTUTTO STRANIERI venduti a prezzi estremamente vantaggiosi

Hacking

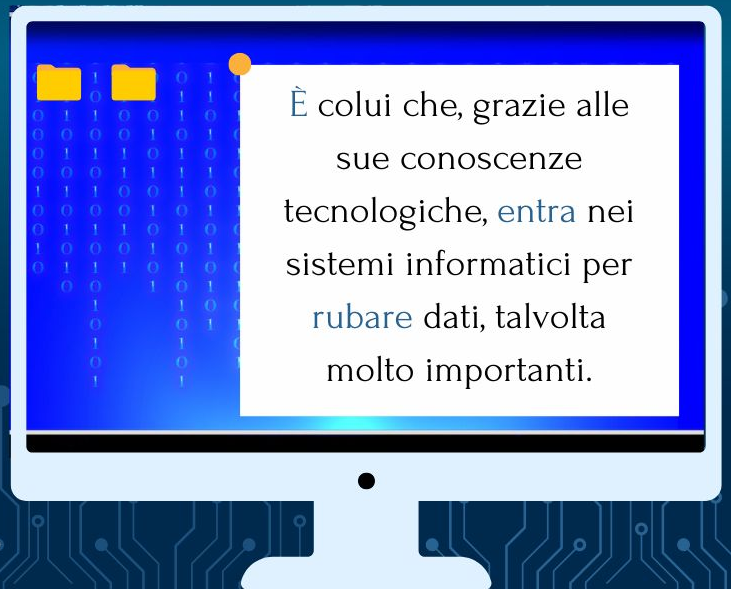
Consigli

Usare firewall, Ovvero quei programmi che **controllano** il nostro rapporto con il mondo esterno e ci **proteggono** da contenuti sospetti

Usando software di cifratura diamo più sicurezza ai messaggi inviati che non **potranno essere letti** così facilmente.

Usare una password sicura.+6 caratteri, senza senso, caratteri speciali, cambiare di volta in volta.

Chi'è un hacker?



È colui che, grazie alle sue conoscenze tecnologiche, entra nei sistemi informatici per rubare dati, talvolta molto importanti.

Money Muling

Il **money mule** è una persona che **trasferisce denaro ottenuto illegalmente** con diversi strumenti di pagamento, molto spesso attraversando diverse nazioni.
Il suo guadagno consiste nel trattenere delle commissioni.





Il Riciclaggio di Denaro è un reato.





PHISHING

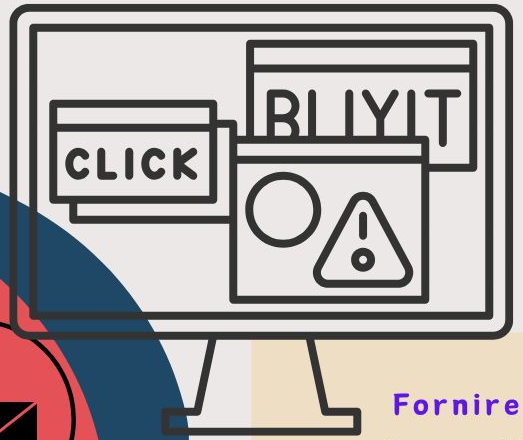




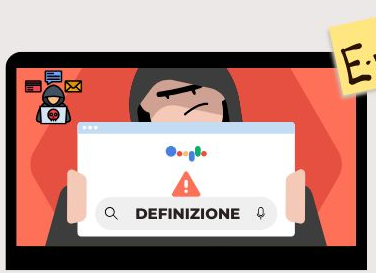
E' una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli

Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio

La forma più diffusa è sempre il classico allegato al messaggio di posta elettronica; oltre i file con estensione .exe, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato .doc .pdf



Attraverso una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce ecc.)



Scopo

Fornire i propri dati riservati di accesso al servizio.



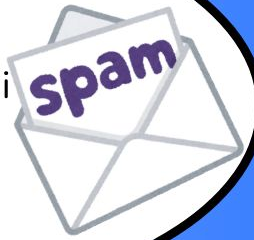




SPAMMING

Cosa é?

L'invio ripetuto, senza consenso del destinatario, di messaggi **di posta elettronica** o newsletter.



Danni subiti dalla vittima



La casella postale della vittima viene **inondata** di posta, che pone seriamente **a rischio il suo funzionamento**

Ricorda...

E' un reato **perseguibile dalla legge**, pertanto se i malfattori persistono, è importante **denunciarli alla polizia postale**.



Come si può prevenire?

- **Installare** un'applicazione o un filtro anti-spam;
- non **condividere** l'e-mail se non necessario;
- non **rispondere** alle e-mail di spam;
- **creare** un account apposito, facilmente eliminabile;
- **leggere** attentamente i moduli sul trattamento della privacy.

PEDOFILIA ONLINE

Fenomeno che è nato con la diffusione di internet e che prevede l'uso del computer e di altri supporti tecnologici analoghi per attività connesse ad interesse pedofilo

PARLANE
con gli psicologi
della **Polizia di Stato**
specializzati in cybercrime

CONSEGUENZE

- suicidio
- problemi psicologici
- depressione
- problemi per il futuro



SI PUO' **PREVENIRE**



COSA SI PUO' FARE?

- **educare** i minori all'uso sicuro della rete
- **controllare** l'attività online dei figli
- **impostare** limiti nell'uso dello smartphone





STOP
ALLA PEDOFILIA ONLINE!!





CYBER HYGIENE



Insieme delle buone regole da seguire per ridurre i rischi online

AGGIORNARE costantemente i sistemi e i software



SCEGLIERE una password sicura ed efficace



PROTEGGERE l' account attivando, nelle impostazioni di sicurezza, l'autenticazione a due fattori o la verifica in due passaggi

NON CLICCARE mai sui link che ricevi per messaggio e non inviare per nessun motivo link e codici ricevuti tramite SMS

CAMBIARE periodicamente la password (ogni 90 giorni)

SALVARE i dati ricorrendo ai backup

NON CONDIVIDERE la password con altre persone

NON UTILIZZARE informazioni riconducibili alla nostra persona o familiari

SOCIAL NETWORK

SONO RETI SOCIALI VIRTUALI CHE CONSENTONO AI PROPRI UTENTI DI INTERAGIRE CON ALTRE PERSONE, SUPERANDO BARRIERE CULTURALI E GEOGRAFICHE





PROTEGGI ULTERIORMENTE IL TUO ACCOUNT ATTIVANDO L'AUTENTICAZIONE A DUE FATTORI O LA VERIFICA IN DUE PASSAGGI

EVITA DI INSERIRE RIFERIMENTI ALLA TUA SFERA PRIVATA

ATTIVA IL CONTROLLO PARENTALE

PROTEGGI I MINORI, LIMITANDO LA PUBBLICAZIONE DELLE LORO FOTO ONLINE

REGOLA LE IMPOSTAZIONI SULLA PRIVACY, RENDENDO IL TUO PROFILO PRIVATO, PER IMPEDIRE AD ESTRANEI DI VISUALIZZARE E SOTTRARRE CONTENUTI RICONDUCIBILI ALLA TUA PERSONA

BISOGNA STARE ATTENTI A FAKE NEWS

EVITA DI CONDIVIDERE FOTO INTIME CON ALTRI UTENTI

LIMITA L'INSERIMENTO DI INFORMAZIONI PRIVATE SUI SOCIAL NETWORK COME DATI ANAGRAFICI

BLOCCA I CONTATTI OSTILI E SEGNALA I POST OFFENSIVI O INADEGUATI

TRATTA GLI UTENTI CON CUI INTERAGISCI CON RISPETTO: RICORDA CHE DIETRO AD UN NICKNAME C'È SEMPRE UNA PERSONA

PUÒ RICEVERE CONSOLAZIONI NEI MOMENTI DIFFICILI

UTILIZZA PASSWORD ALFANUMERICHE COMPLESSE

EVITA DI CONDIVIDERE LA TUA POSIZIONE IN TEMPO REALE

NON CLICCARE MAI SUI LINK SOSPETTI RICEVUTI CON MESSAGGIO PRIVATO





CYBERSTALKING

Forma di **stalking online** che può essere punita anche penalmente.







Il CYBER STALKER esiste "solo" nella realtà virtuale.

Le ripercussioni sono però reali.

Il persecutore può essere sia uomo che donna, di qualsiasi età ed estrazione sociale.

Divulga il minor numero di informazioni personali

Non rispondere a messaggi provocatori





Se alcune conversazioni online ti mettono a disagio **parlane** con qualcuno

Consenti solo a persone che conosci la visualizzazione del tuo profilo

Segnala ogni tipo di sospetto





SOCIAL NETWORK

MESSAGGISTICA ISTANTANEA

E-MAIL











LA RETE
MIGLIORA LA VITA
MA E' NECESSARIO
NAVIGARE IN SICUREZZA









