USCITE DI SICUREZZA

USCITE DI SICUREZZA

INCONTRO TRE

NAVIGAZIONE E ACQUISTI ONLINE

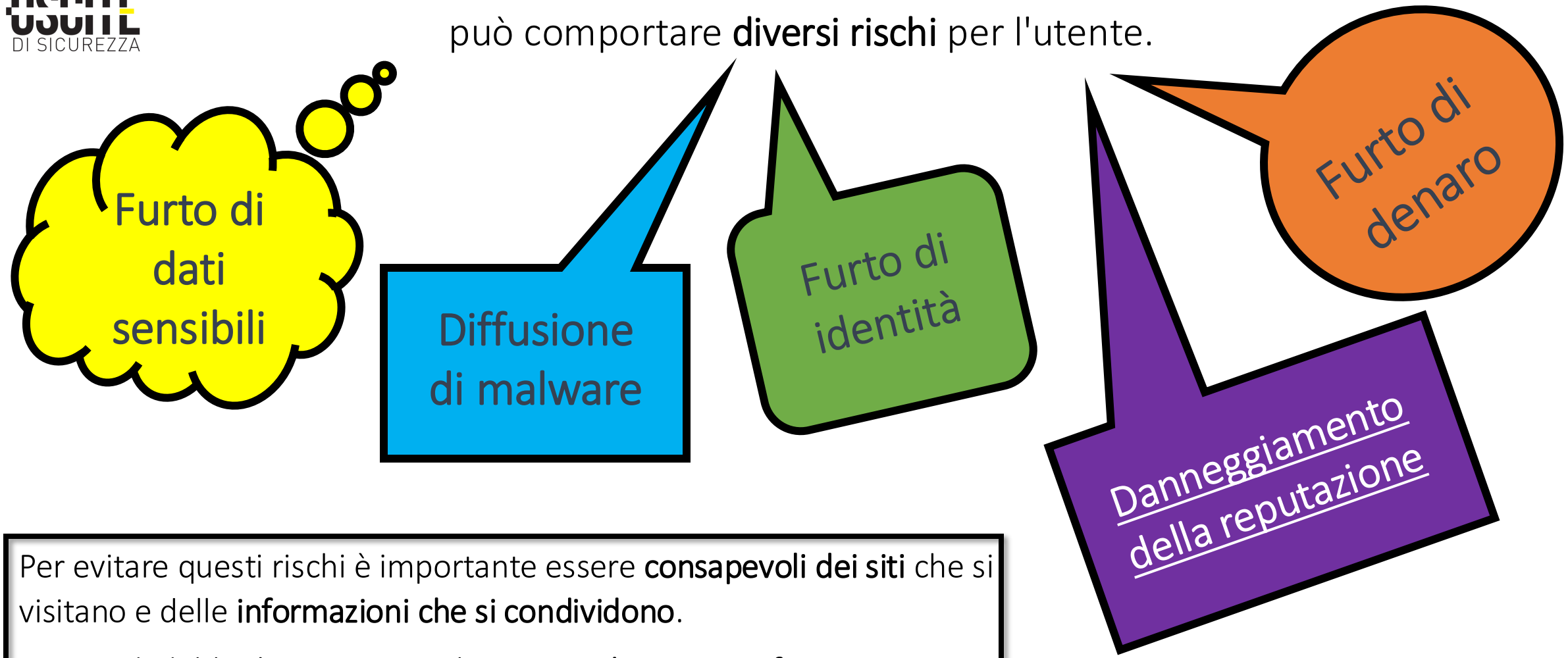
NAVIGARE A VISTA

Per navigare sicuri su internet e, quindi, non temere di furti di dati, di password, di soldi o di pericoli da malware, virus e hacker è necessario adottare alcune **precauzioni**:

1. **Proteggere gli account con nuove password** → Per account importanti è bene **cambiare password spesso**;
2. **Controllare sempre i permessi delle App** → di solito le applicazioni richiedono le autorizzazioni quando le si apre per la prima volta, ma è bene **verificare nel tempo che queste non siano variate**;
3. **Scoprire cosa i Social network "sanno"** → I Social utilizzano le informazioni personali principalmente per fornire una pubblicità mirata, ma è bene rimanere al corrente di quali informazioni acquisiscono da voi e **controllare il flusso** attraverso la **gestione delle impostazioni della privacy;**
4. **Cancellare la cronologia di navigazione** → I Browser Web monitorano le attività passate, perciò è bene **cancellare ogni settimana la cronologia e i cookies**;
5. **Accesso HTTPS** → La connessione **HTTPS** aggiunge un ulteriore livello di **sicurezza crittografica** al login rendendo più difficile sottrarre informazioni personali. Per verificare la presenza di una connessione HTTPS bisogna **controllare la presenza di un lucchetto nella barra indirizzi del browser** o **accertarsi che l'URL inizi con HTTP**;
6. **Evitare le truffe sui siti eCommerce** → Quando fai degli acquisti online **non salvare mai i codici delle tue carte di credito** nel tuo browser;
7. **Tienere gli estranei fuori dalla rete Wi-Fi** → Non dare mai la password del tuo Wi-Fi a chi non conosci;
8. **Non collegarsi ad un Wi-Fi pubblico** → Una volta connessi, condividerete la rete con altre persone, alcune delle quali potrebbero così accedere alle tue attività online. Evitate, soprattutto, di fare acquisti online utilizzando reti pubbliche;
9. **Eseguire il backup del computer** → Fare periodicamente un completo di backup è una sicurezza in più contro hacker e virus e protegge dal trauma di eliminare accidentalmente i file.

NAVIGAZIONE E SITI FAKE

Un **sito web falso**, anche conosciuto come sito "**phishing**", può comportare **diversi rischi** per l'utente.



Per evitare questi rischi è importante essere **consapevoli dei siti** che si visitano e delle **informazioni che si condividono**.

In caso di dubbi, è sempre meglio **evitare di inserire informazioni personali** o di scaricare file da tale sito web.

INDIVIDUARE I SEGNALI DI UN SITO FAKE

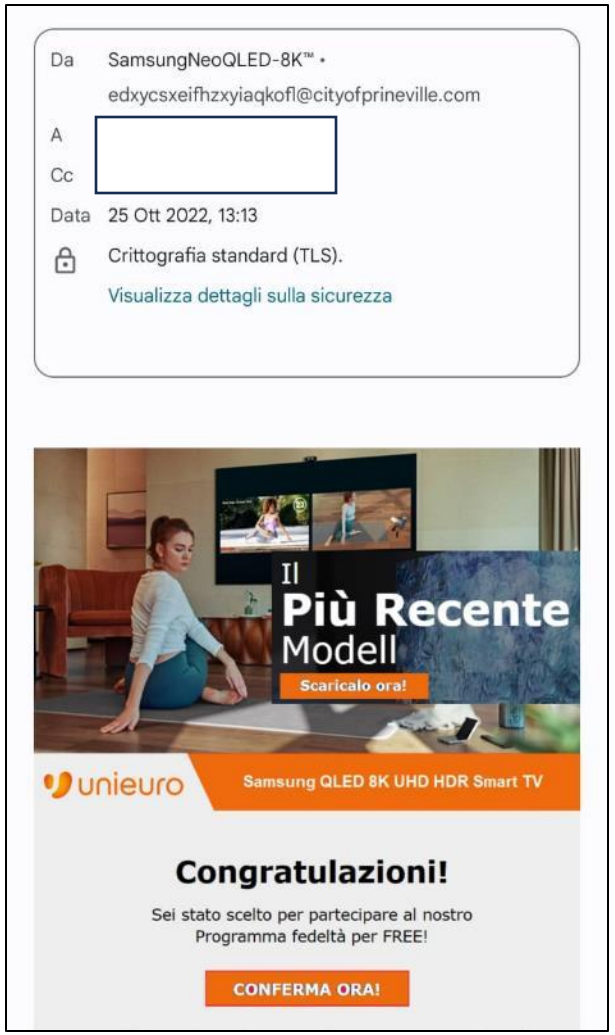
Controllare il tipo di connessione e il dominio: accertarti che i siti che visiti utilizzino il protocollo **HTTPS** (*HyperText Transfer Protocol over Secure Socket Layer*), che indica la presenza di una **connessione sicura**.

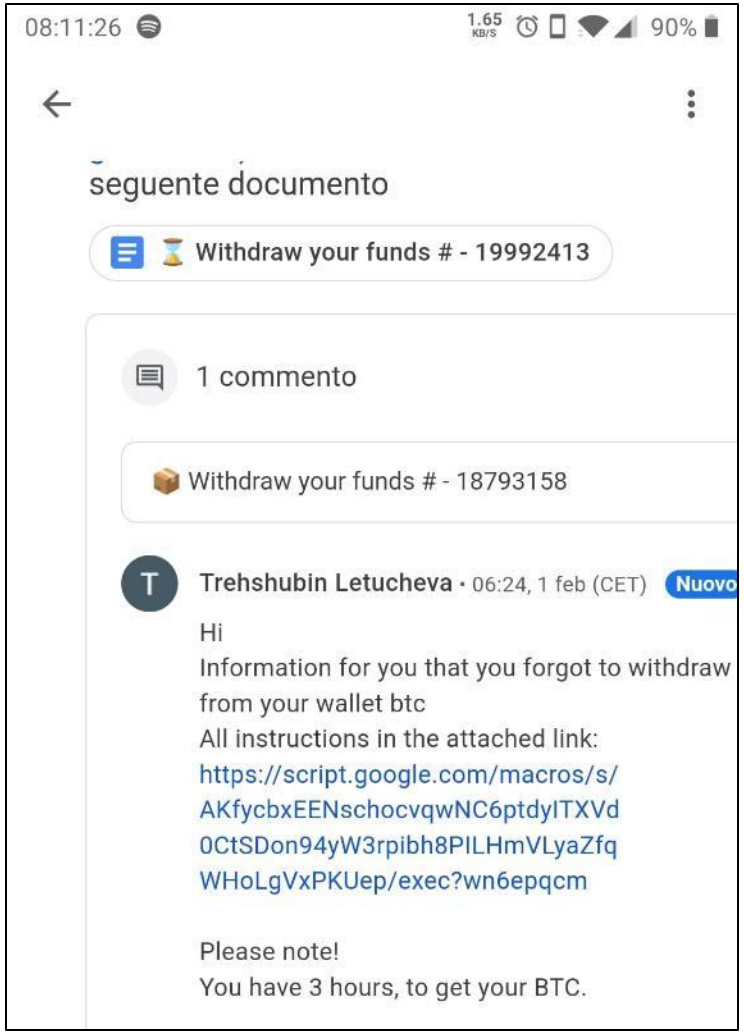
Verificare la Web Reputation di un sito, ovvero la reputazione che gli utenti del Web hanno dello stesso mediante le recensioni che ne fanno.

Controllare che un sito non sia pericoloso mediante un buon software **antivirus**.

Verificare l'assenza di minacce tramite l'URL del portale: https://www.virustotal.com/gui/home/upload

SCOVA GLI INDIZI



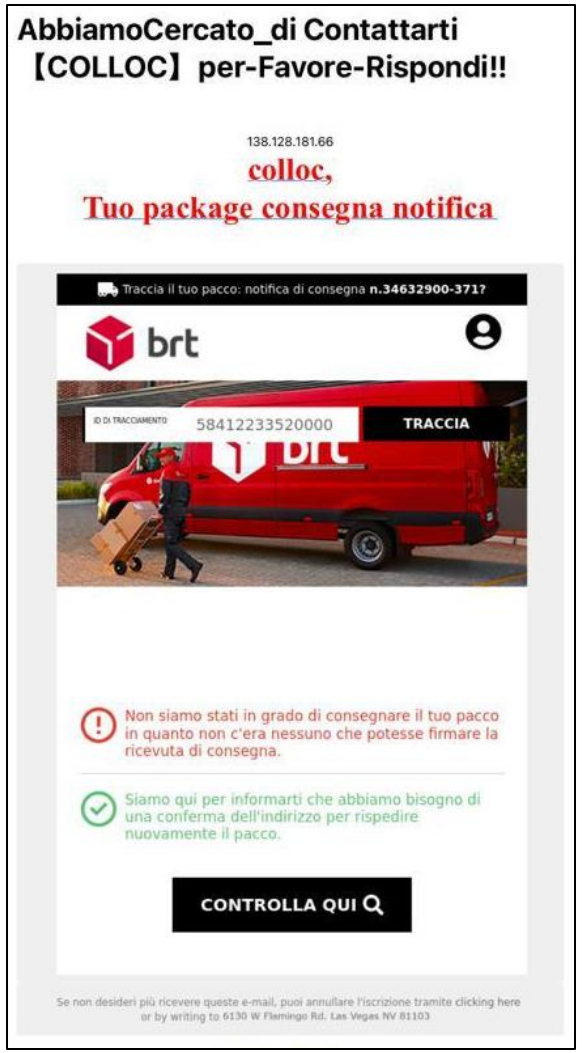


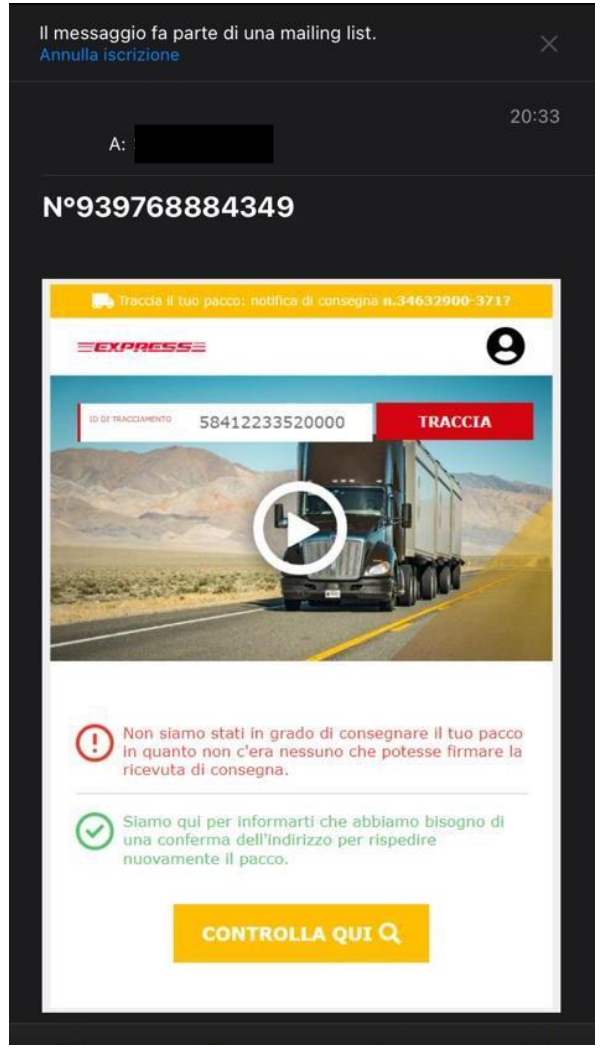
DA COSA È POSSIBILE CAPIRE CHE QUESTI SONO MESSAGGI E E-MAIL FAKE?

PROVATE, SINGOLARMENTE O IN GRUPPO!

SCOVA GLI INDIZI

DA COSA È POSSIBILE CAPIRE CHE QUESTI SONO MESSAGGI ED E-MAIL FAKE?





PROVATE, SINGOLARMENTE O IN GRUPPO!

USCITE DI SICUREZZA

ACQUISTI ONLINE

COSA COMPRI ONLINE?

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/alrh9b4k9y5w

PAY SAFE

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/aluw5jtomfpm

"CONSIGLI PER GLI ACQUISTI" ONLINE IN SICUREZZA

LA PAROLA ALL'ESPERTO

Progettista Paolo Bizzotto

10 BUONE PRASSI DI SICUREZZA INFORMATICA

1. Cambiare le password predefinite: molte periferiche di rete vengono fornite con password predefinite. Queste sono facilmente scopribili e devono essere cambiate.
2. Aggiornare regolarmente i dispositivi: gli aggiornamenti includono spesso *patch* di sicurezza importanti. Bisogna assicurarsi che tutti i dispositivi siano aggiornati alla versione più recente del *software*.
3. Utilizzare una rete Wi-Fi sicura: utilizzare la crittografia WPA2 per proteggere la rete Wi-Fi. Evitare di utilizzare la crittografia WEP, che è facilmente violabile.
4. Disattivare la connessione automatica alle reti Wi-Fi pubbliche: queste reti sono spesso non sicure e possono esporre i dati a rischio di accesso non autorizzato.
5. Utilizzare software antivirus: per proteggere i dispositivi domestici da *virus* e *malware*.
6. Utilizzare la crittografia: per proteggere i dati sensibili e assicurarsi che le informazioni personali siano sempre criptate quando si inviano o si ricevono.
7. Evitare di condividere informazioni personali online: come numeri di telefono, indirizzi e-mail, informazioni finanziarie o informazioni di login sui social media e sui siti web non affidabili.
8. Fare attenzione alle e-mail di *phishing*: queste cercano di ingannare l'utente a fornire informazioni personali o a cliccare su un link dannoso.
9. Utilizzare un firewall: per proteggere la rete domestica da accessi non autorizzati.
10. Configurare correttamente le impostazioni di *privacy* sui dispositivi: per limitare l'accesso a informazioni personali e sensibili.

USCITE DI SICUREZZA

Per i contenuti si ringrazia:

Fabio C.

Silvio C.

Promosso e finanziato da:

Città di Torino

Progetto realizzato da:

ismel

orso

MAGAZZINI Oz

UTILE PER IL SOCIALE