APVE in rete

Modulo 4 – Sicurezza on line

Programma di formazione informatica per i soci Apve di Roma

aprile 2017

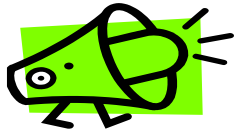
Agenda

- Obiettivo della sicurezza

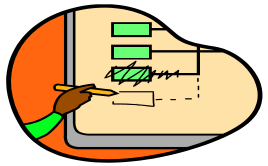
- Comportamenti degli utenti
  - Phishing, virus e altre minacce
  - Occhio alle bufale
  - Sui Social (Facebook e Linkedin)
  - In mobilità
  - Carte di credito: ecco come evitare le truffe
  - IoT

Obiettivo della sicurezza

Proteggere le informazioni da atti non autorizzati:



Divulgazione



Alterazione

Disponibilità

R

Riservatezza

I

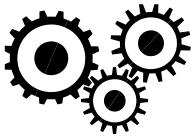
Integrità

D

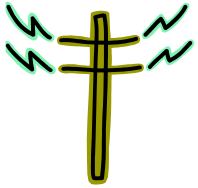
Disponibilità

– In tutti gli stadi in cui viene:

Memorizzata



Processata



Trasmessa

Comportamenti degli utenti

Phishing, virus e altre minacce

- Non fidarti mai di mail che contengono richieste di azione immediata e cercano di allarmarti minacciando gravi conseguenze, quali la chiusura di un account, la disabilitazione di una carta di credito o addirittura un'azione giudiziaria.

- Molte mail di phishing infatti, ricorrono a questo espediente simulando nella grafica e nel contenuto la provenienza da aziende o istituzioni che ti sono ben note, come ad esempio la tua banca o enti pubblici, per cercare di carpirti dati e informazioni.

esempio phishing.msg

esempio phishing 1.gif

E' nata la nuova Acea Energia digitale!.msg

You have notifications pending .msg

Comunicazione importante conto bloccato!.msg

Comportamenti degli utenti

Occhio alle bufale

La rete e le caselle di posta sono piene di “bufale”, ovvero di messaggi ingannevoli inviati agli utenti tramite mail o banner pubblicitari a scopi fraudolenti, assimilabili al phishing. **Una bufala può contenere richieste di denaro e di informazioni personali o istruzioni per interventi sul PC per la rimozione di virus in realtà inesistenti,** che una volta eseguite, potrebbero causare danni anche gravi, come la cancellazione di file necessari.

- Come riconoscere le “bufale”. Contengono tipicamente:
  - minaccia di conseguenze tragiche se non vengono eseguite le azioni indicate nel messaggio;
  - promessa di denaro, regali e buoni sconto, a fronte di determinate azioni, come fornire i dati personali e quelli della propria carta di credito;
  - segnalazioni di malattie, spesso di bambini, con richiesta di donazioni;
  - l’invito a diffondere la mail, creando una “catena di Sant’Antonio”.

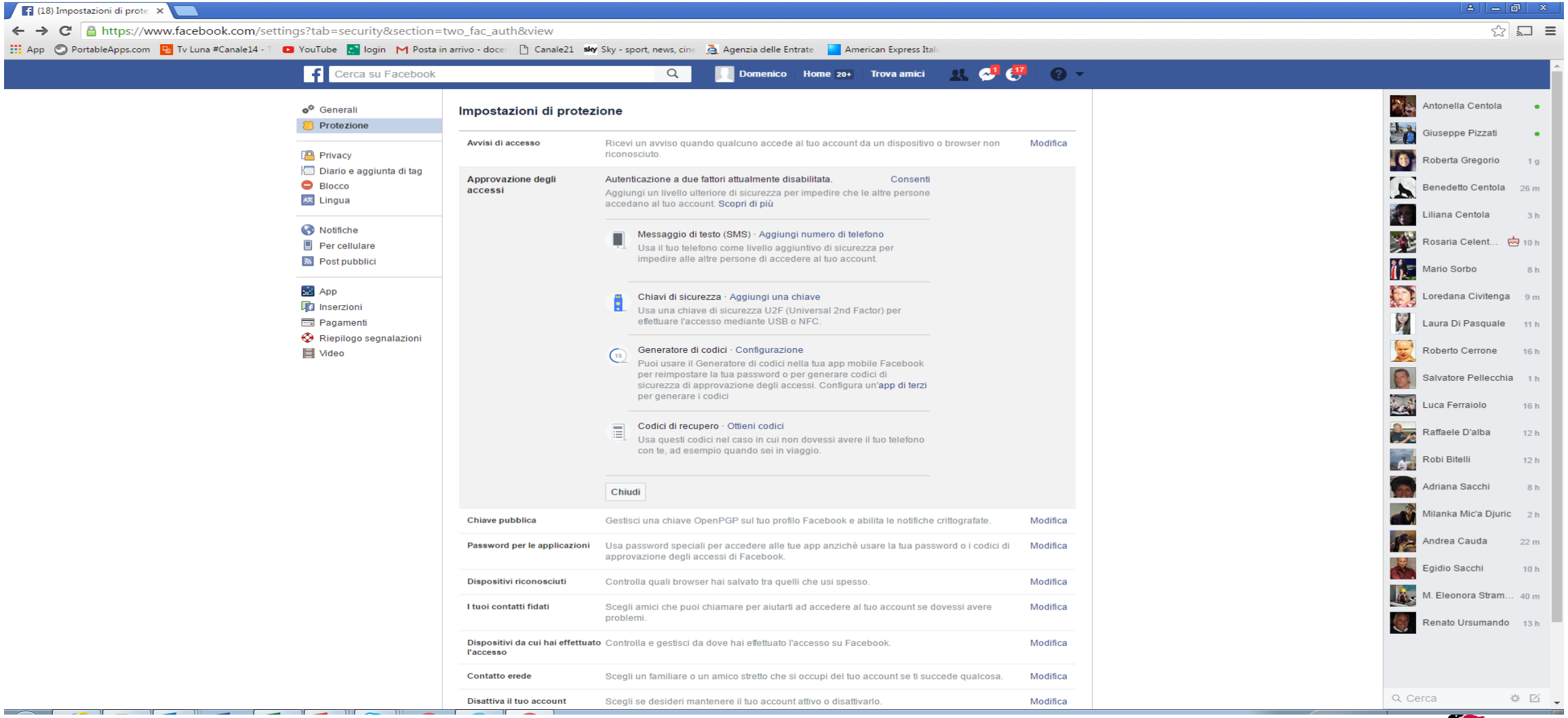
esempio bufala.msg

Comportamenti degli utenti

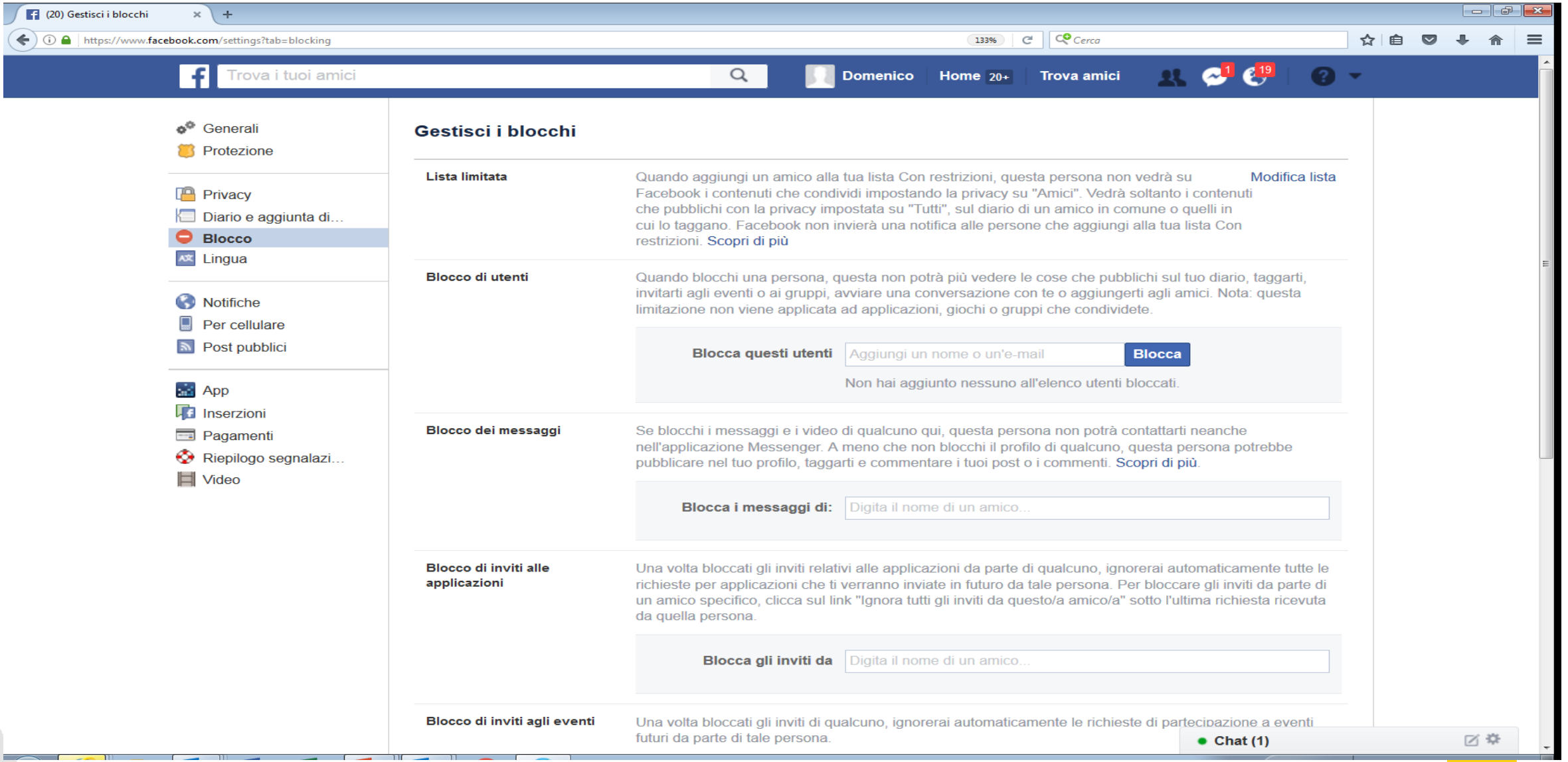
Sui social - Facebook

- Evita di utilizzare il profilo Facebook per accedere ad altri siti, che in questo caso potranno postare sul diario e leggere le informazioni personali.
- Valuta la possibilità di impostare un codice di sicurezza da ricevere via cellulare nel caso di accesso al tuo account da un PC o uno smartphone sconosciuto. E’ semplice, basta andare in: "Impostazioni -> Protezione -> Approvazione degli accessi"
- Controlla regolarmente le impostazioni Privacy. Oltre a scegliere il livello di apertura o chiusura del tuo profilo, ricordati che cliccando su "Blocco" puoi impedire l’accesso al tuo profilo a persone indesiderate, mentre cliccando su "Diario e aggiunta di tag" puoi impostare la visibilità del tuo diario e gestire i tag col tuo nome aggiunti dagli altri utenti.

Comportamenti degli utenti



Comportamenti degli utenti



Comportamenti degli utenti

Tutte le volte che hai il dubbio che il tuo account sia stato violato procedi a un cambio psw

- Scegli psw robuste (lunghe almeno 8 caratteri e usa almeno un carattere speciale e/o un carattere numerico)
- Non riutilizzare le ultime 6 psw
- Non usare la stessa psw per tutti i siti
- Memorizza anche la domanda segreta che scegli quando definisci un account
- Attenzione ai promemoria con le password

- Evita di inserire una psw errata per più di tre tentativi
- Non lasciare mai incustodito il tuo pc con documenti o sessioni di lavoro aperte
- Configurare il pc in modo che si attivi lo screensaver dopo un intervallo di tempo (es. 15 min)

Comportamento utenti

Sui social – Linkedin

- Un profilo LinkedIn può fornire molte informazioni utili per un cyber attacco, quali nome, ruolo aziendale, indirizzo email e progetti aziendali. Queste informazioni possono fornire le esche per attacchi di phishing mirati, tipicamente tramite l'indirizzo email associato all'account LinkedIn, o di social engineering.

- Poni la massima attenzione a ciò che inserisci nel profilo professionale: non pubblicare mai informazioni riguardanti Eni relative a progetti, iniziative, dati confidenziali o comunque non di pubblico dominio.

- Fai attenzione alle mail di phishing: anche in caso di mail apparentemente ricevute tramite il profilo LinkedIn in cui si invita a cliccare su un link, è necessario verificare la congruenza tra il link "apparente" e il collegamento vero.

Comportamenti degli utenti

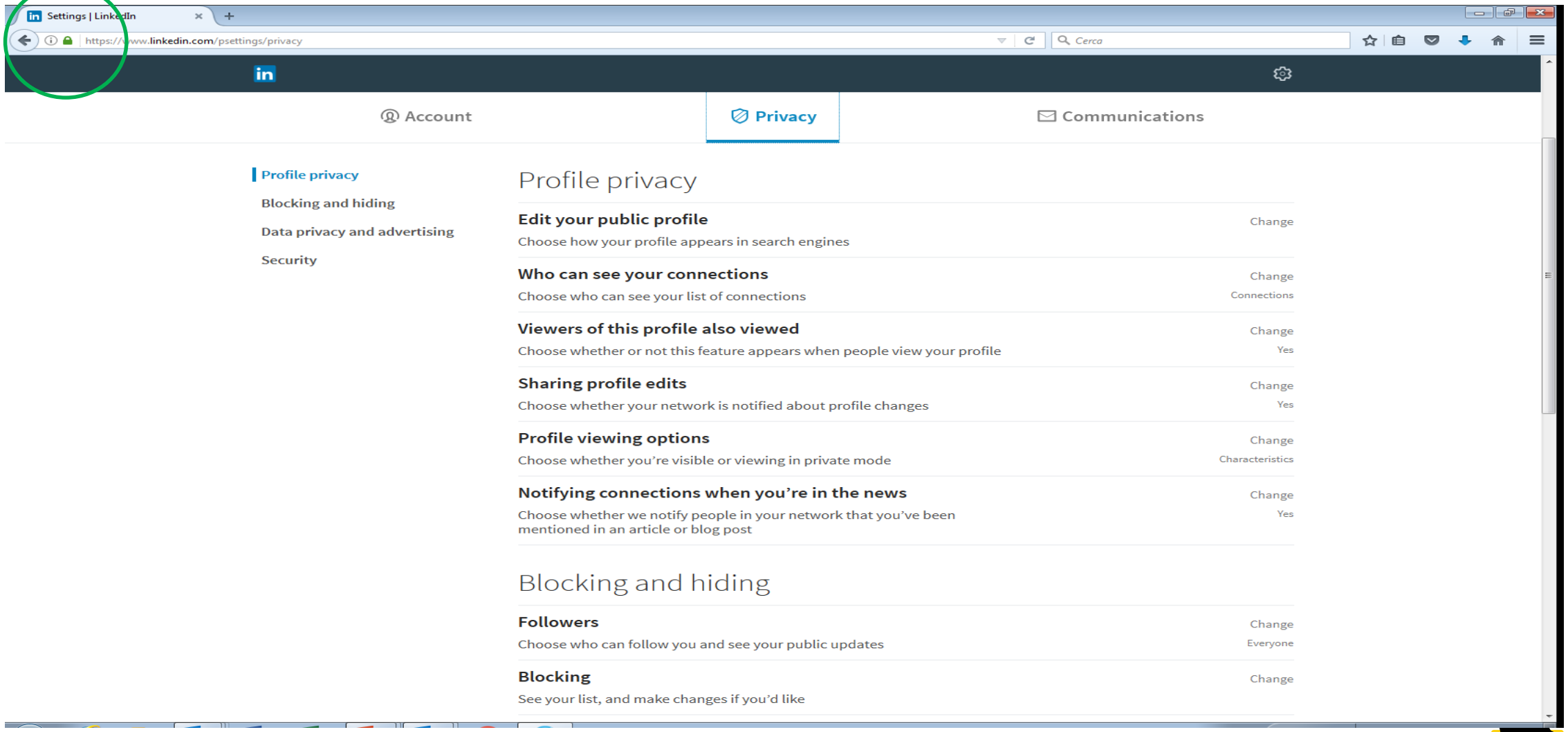
Sui social - Linkedin

- Attiva la verifica in due passaggi: per assicurare una maggiore protezione del tuo account LinkedIn da accessi abusivi, ti consigliamo di attivare, tramite l'opzione "Protezione" nel profilo Privacy, il processo di verifica in due passaggi. Se attivato, in caso di primo accesso da un dispositivo sconosciuto, viene richiesto un codice di controllo che viene inviato via SMS al numero di cellulare impostato in fase di configurazione email associato all'account LinkedIn.

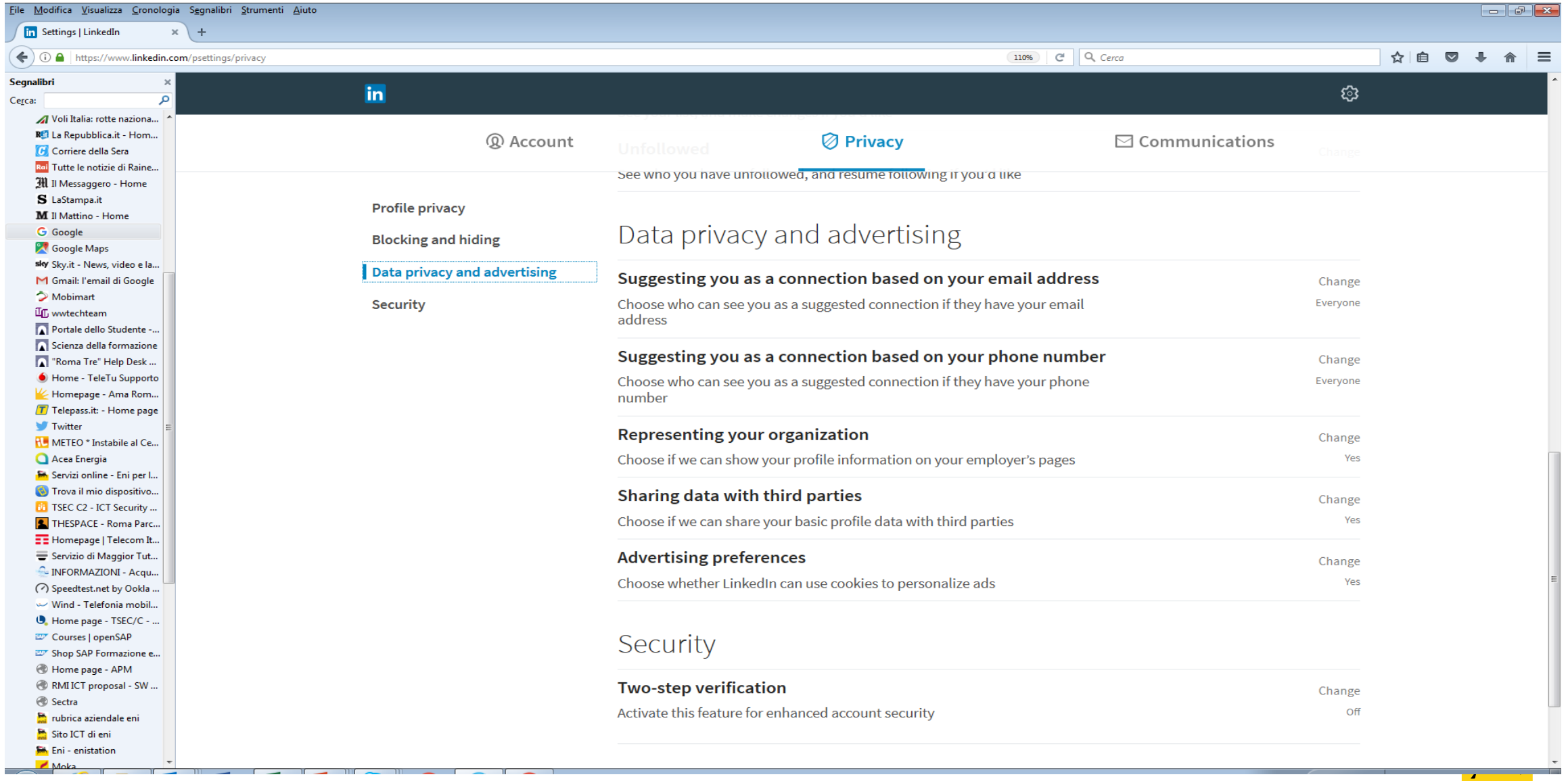
- Configura correttamente il tuo profilo: tramite le impostazioni Privacy del profilo è possibile stabilire chi può vedere i collegamenti, chi può vedere gli aggiornamenti del profilo, se nascondere il profilo sulle pagine del datore di lavoro, se far sapere alle persone nella propria rete se il proprio nome è citato in un articolo o un blog e se LinkedIn può condividere con terzi le informazioni del profilo.

Comportamenti degli utenti

Sito sicuro



Comportamenti degli utenti



Comportamenti degli utenti

In mobilità

Le app che installiamo nei nostri smartphone possono essere un ricettacolo di virus di varia natura e addirittura accedere e trasmettere informazioni personali a insaputa del possessore del dispositivo, oltre a consumare memoria e batteria e generare traffico in background.

- **Presta sempre attenzione alle funzioni a cui può avere accesso un'app**, segnalate in fase di installazione, e non attivare il servizio di geolocalizzazione se non è necessario. Non attivare Bluetooth se non è necessario.

- **Limita il traffico dati in background.** Le App possono generale moli considerevoli di traffico dati in background, causando un rapido esaurimento del pacchetto dati mensile o costi anche molto elevati in caso di contratti a consumo. Per evitare spiacevoli sorprese è opportuno abilitare le funzioni di limitazione del traffico dati in background, nonché disabilitare le funzioni di roaming all'estero.

- **Installa solo App sicure.** E' opportuno installare solo le app di cui si ha realmente bisogno e solo da fonti affidabili, come iTunes per i dispositivi Apple e Google Play per i dispositivi Android. Evita le app che sono state appena pubblicate, scaricate da poche persone e che hanno ricevuto pochi commenti positivi

Comportamenti degli utenti

In mobilità

Quando viaggi

PRIMA DI PARTIRE

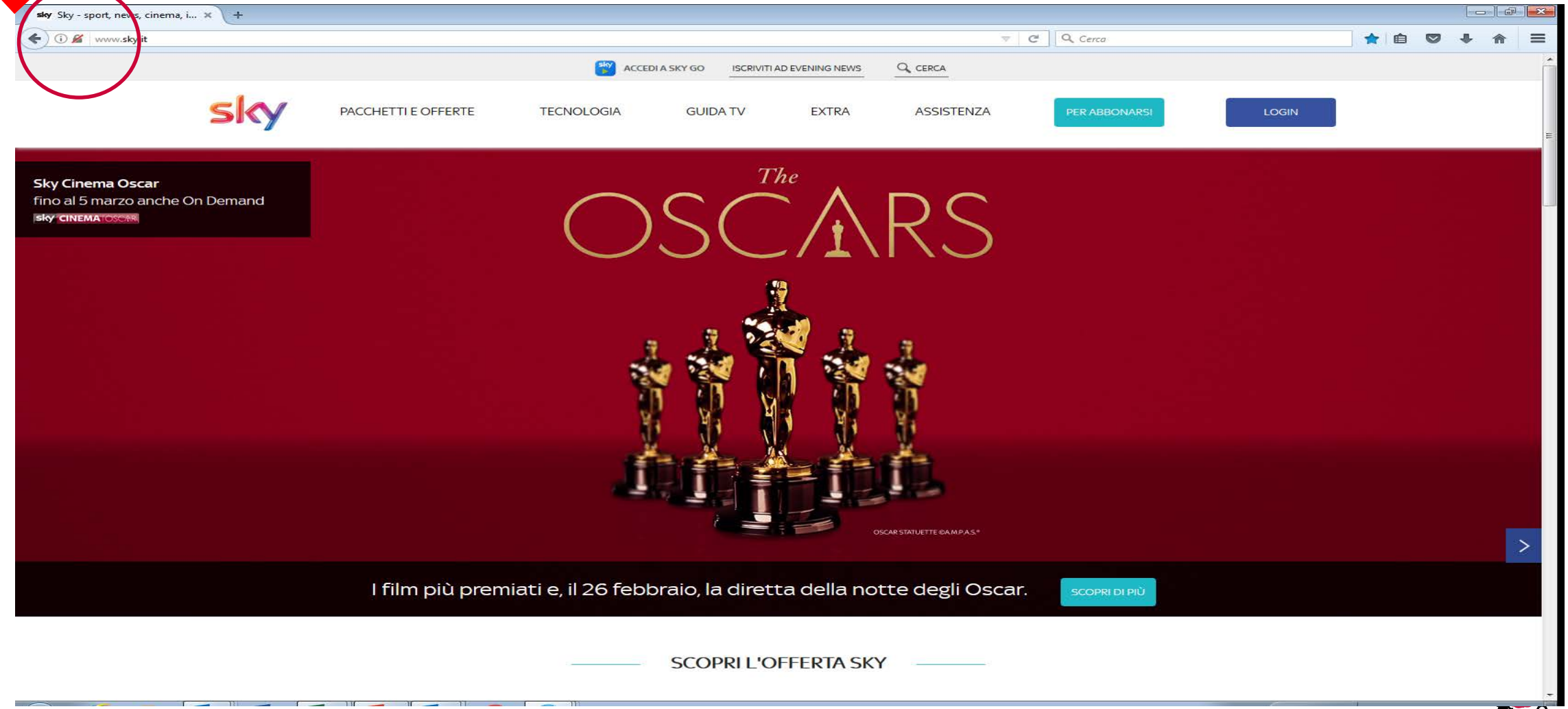
- Verifica il piano tariffario del telefono all'estero.
- Installa un software di tracciamento sul dispositivo in modo da poter capire dove si trova, in caso di perdita o furto.
- Assicurati che l'antivirus sia aggiornato.
- Imposta una password robusta su tablet, smartphone e computer.
- Esegui un salvataggio completo dei dati e delle configurazioni dei dispositivi.

DURANTE IL VIAGGIO

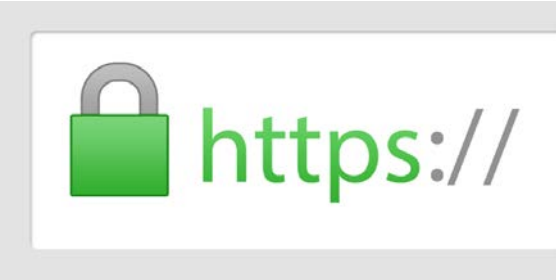
- Non lasciare mai i dispositivi incustoditi.
- Se ti trovi a dover utilizzare un PC pubblico, non accedere a nessun servizio che richieda l'autenticazione con utente e password.
- Se utilizzi un accesso a un Wi-Fi pubblico, assicurati che le connessioni siano protette da crittografia. Lo puoi capire se prima dell'indirizzo compare la sigla "https" o un lucchetto come questo

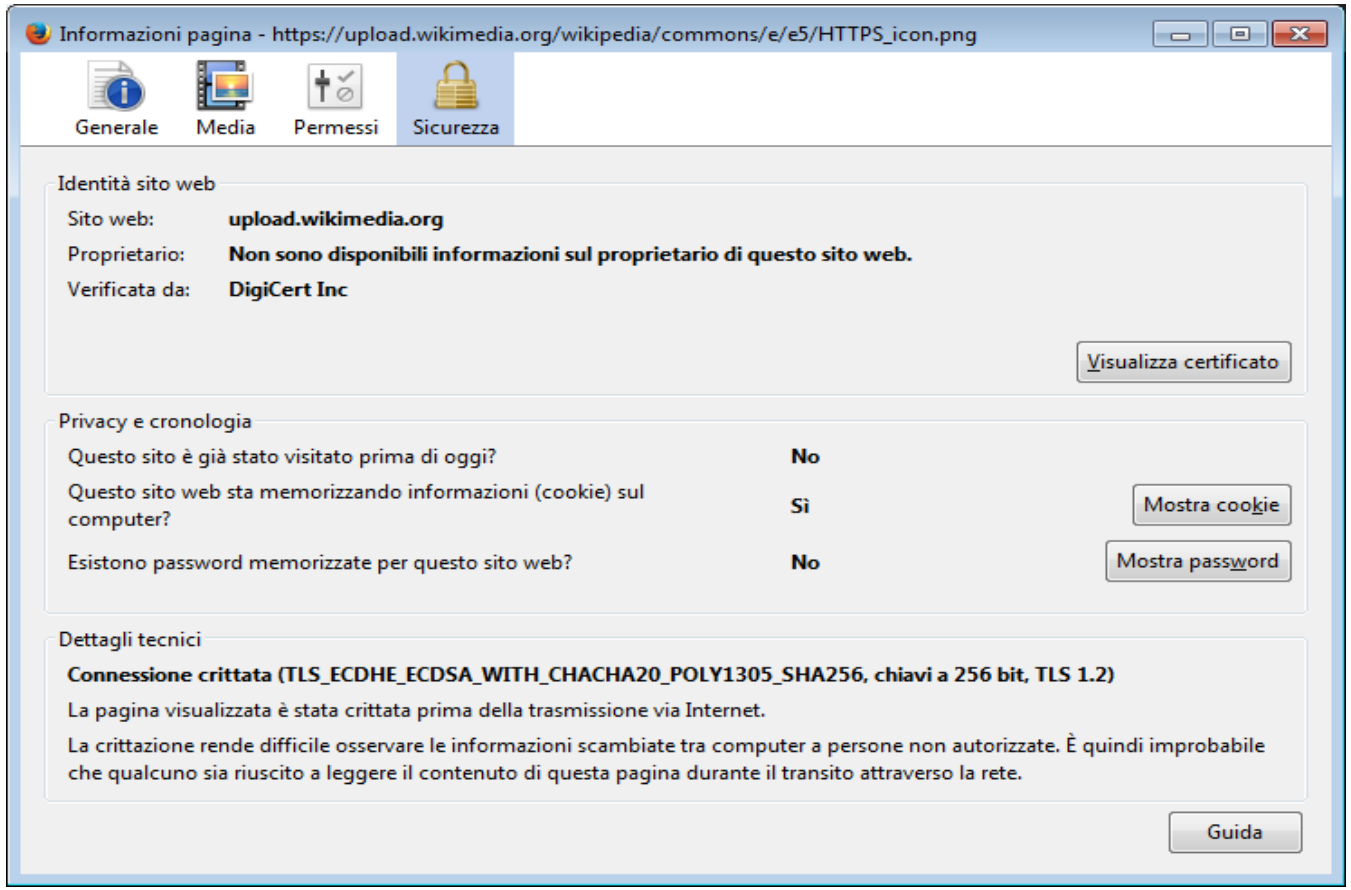
Comportamenti degli utenti

Sito non sicuro



Comportamenti degli utenti





Informazioni sui cookie

Categorie dei cookie

I cookie sono stringhe di testo di piccole dimensioni (formate in genere da lettere e numeri) che consentono ad un sito di riconoscere un particolare dispositivo o browser; infatti, tali file di testo vengono inviati da un sito web al browser utilizzato dall'utente per la navigazione, successivamente vengono memorizzati sul suo dispositivo (es. Computer, Tablet, Smartphone, ecc.) e ritrasmessi al medesimo sito durante la successiva visita dell'utente.

- **cookie di sessione**, cancellati immediatamente alla chiusura del browser di navigazione;
- **cookie persistenti**, che rimangono all'interno del dispositivo continuando ad operare anche successivamente alla chiusura del browser e fino al decorso di un determinato periodo di tempo;
- **cookie di prima parte**, generati e gestiti direttamente dal soggetto gestore del sito web sul quale l'utente sta navigando;
- **cookie di terza parte,** generati e gestiti da soggetti diversi dal gestore del sito web sul quale l'utente sta navigando (in forza, di regola, di un contratto tra il titolare del sito web e la terza parte).

Categorie funzionali:

- **cookie tecnici** *non richiedono consenso, ma è necessario che l'utente sia informato*
- **cookie di profilazione** *richiedono consenso*

da www.acea.it

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3585077

Comportamenti degli utenti

Carte di credito: ecco come evitare le truffe

1. Le carte ed i loro codici segreti non devono mai essere conservati insieme;
2. Se possibile memorizzare i codici e, in ogni caso, non riscriverli mai su bigliettini o foglietti di carta conservati nel portafogli;
3. Non rivelare ad alcuno i codici associati alle carte di pagamento, si tratta di dati rigorosamente personali e non può accadere che ci siano richiesti via e-mail ;
4. Scegliere una carta di pagamento che offra il servizio gratuito di informazione delle operazioni tramite sms;
5. Prestare attenzione a non essere osservati durante l'operazione di digitazione del codice segreto PIN (Personal Identification Code);
6. Controllare tutti i movimenti della carta ogni volta che viene data in mano ad un esercente per l'operazione di pagamento;
7. Conservare gli scontrini dei prelevamenti e dei pagamenti effettuati con carta di credito, in modo da poter verificare dall'estratto conto, le somme addebitate e quelle effettivamente spese;
8. Tenere sempre a portata di mano il numero verde dell'istituto emittente per poter bloccare la carta in caso di necessità;
9. In caso di acquisti online, utilizzare preferibilmente una carta prepagata, ma anche una normale carta di credito è più sicura di un bonifico;
10. Non inviare mai denaro contante e rifiutarsi di ricaricare la carta prepagata del venditore.

Comportamenti degli utenti

IoT (*Internet of things*)

- **Connetti alla rete Wi-FI solo ciò che serve**: il modo più semplice per rendere sicuro un dispositivo è non connetterlo a Internet, se non è strettamente indispensabile.
- **Come per il tuo PC, assicurati di mantenere aggiornati anche i dispositivi IoT**, abilitando le funzionalità di aggiornamento automatico, ove disponibili.
- **Fai attenzione alle password:** utilizza password complesse, difficili da identificare.
- **Acquista prodotti e servizi solo di aziende con una buona reputazione**, verificando le clausole Privacy e rifiutando quelle che prevedono la cessione a terzi dei dati.
- **Scarica le applicazioni per il vostro dispositivo solo da piattaforme affidabili**, come Google Play o App Store.