



APVE in rete

Modulo 4 – Sicurezza on line

Programma di formazione informatica per i soci Apve di Roma

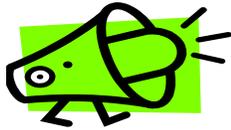
aprile 2017

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

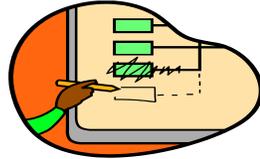
Proteggere le informazioni da atti non autorizzati:



Divulgazione



Riservatezza



Alterazione



Integrità



Disponibilità

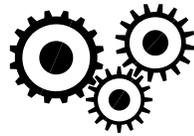


Disponibilità

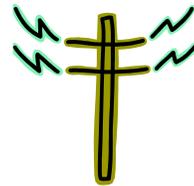
– In tutti gli stadi in cui viene:



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”.



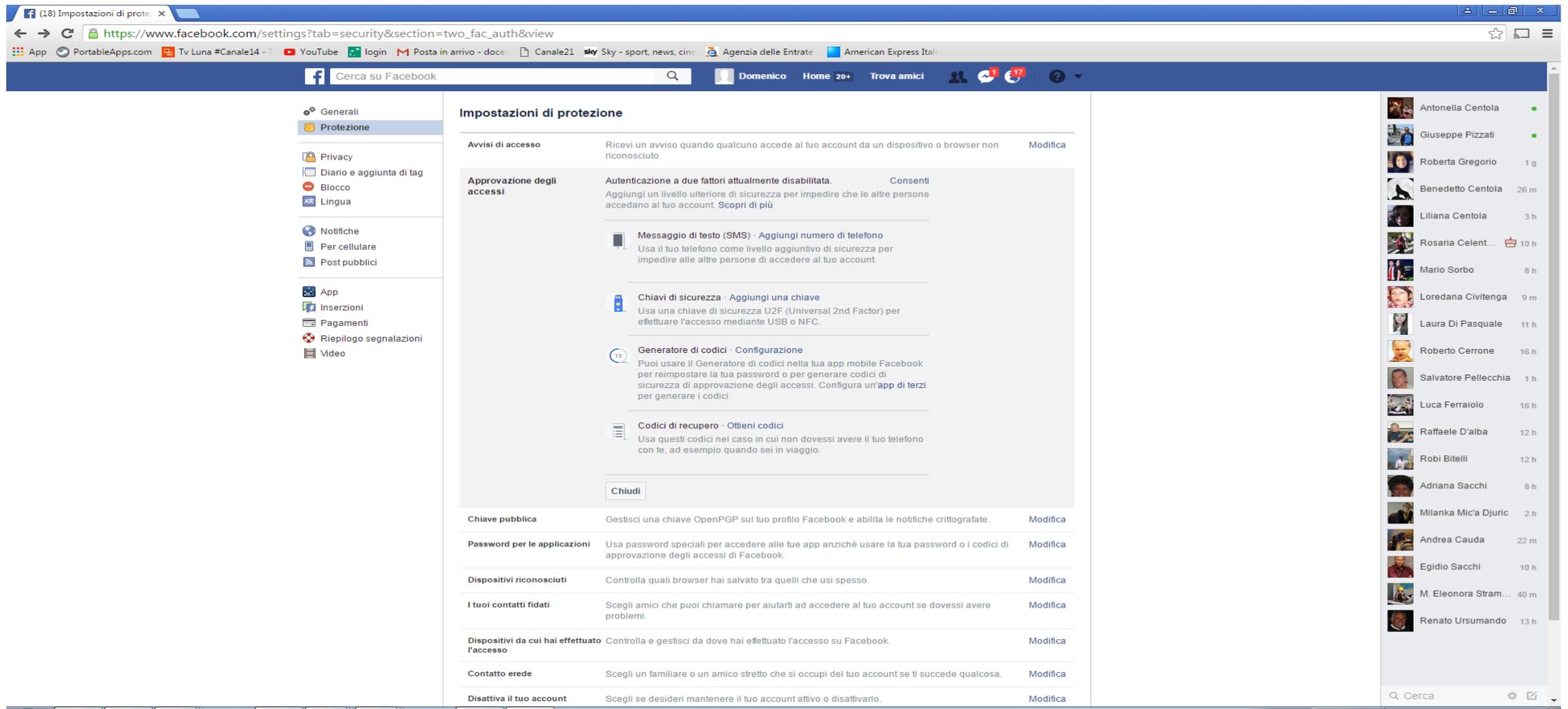
esempio bufala.msg

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



The image shows a screenshot of a web browser displaying the Facebook security settings page. The browser's address bar shows the URL: https://www.facebook.com/settings?tab=security§ion=two_fac_auth&view. The page title is "Impostazioni di protezione".

On the left side, there is a navigation menu with the following items: "Generali", "Protezione" (highlighted), "Privacy", "Diario e aggiunta di tag", "Blocco", "Lingua", "Notifiche", "Per cellulare", "Post pubblici", "App", "Inserzioni", "Pagamenti", "Riepilogo segnalazioni", and "Video".

The main content area is titled "Impostazioni di protezione" and contains several sections:

- Avvisi di accesso:** Ricevi un avviso quando qualcuno accede al tuo account da un dispositivo o browser non riconosciuto. [Modifica](#)
- Approvazione degli accessi:** Autenticazione a due fattori attualmente disabilitata. [Consenti](#)
Aggiungi un livello ulteriore di sicurezza per impedire che le altre persone accedano al tuo account. [Scopri di più](#)
- Messaggio di testo (SMS) - Aggiungi numero di telefono:** Usa il tuo telefono come livello aggiuntivo di sicurezza per impedire alle altre persone di accedere al tuo account.
- Chiavi di sicurezza - Aggiungi una chiave:** Usa una chiave di sicurezza U2F (Universal 2nd Factor) per effettuare l'accesso mediante USB o NFC.
- Generatore di codici - Configurazione:** Puoi usare il Generatore di codici nella tua app mobile Facebook per reimpostare la tua password o per generare codici di sicurezza di approvazione degli accessi. Configura un'app di terzi per generare i codici.
- Codici di recupero - Ottieni codici:** Usa questi codici nel caso in cui non dovessi avere il tuo telefono con te, ad esempio quando sei in viaggio.
- Chiave pubblica:** Gestisci una chiave OpenPGP sul tuo profilo Facebook e abilita le notifiche crittografate. [Modifica](#)
- Password per le applicazioni:** Usa password speciali per accedere alle tue app anziché usare la tua password o i codici di approvazione degli accessi di Facebook. [Modifica](#)
- Dispositivi riconosciuti:** Controlla quali browser hai salvato tra quelli che usi spesso. [Modifica](#)
- I tuoi contatti fidati:** Scegli amici che puoi chiamare per aiutarti ad accedere al tuo account se dovessi avere problemi. [Modifica](#)
- Dispositivi da cui hai effettuato l'accesso:** Controlla e gestisci da dove hai effettuato l'accesso su Facebook. [Modifica](#)
- Contatto erede:** Scegli un familiare o un amico stretto che si occupi del tuo account se ti succede qualcosa. [Modifica](#)
- Disattiva il tuo account:** Scegli se desideri mantenere il tuo account attivo o disattivarlo. [Modifica](#)

On the right side, there is a list of friends with their profile pictures and names, including: Antonella Centola, Giuseppe Pizzati, Roberta Gregorio, Benedetto Centola, Lilliana Centola, Rosaria Celent..., Mario Sorbo, Loredana Civitenga, Laura Di Pasquale, Roberto Cerrone, Salvatore Pellecchia, Luca Ferraiolo, Raffaele D'alba, Robi Bitelli, Adriana Sacchi, Milanka Mic'a Djuric, Andrea Cauda, Egidio Sacchi, M. Eleonora Stram..., and Renato Ursumando.



Comportamenti degli utenti

The screenshot shows the Facebook 'Gestisci i blocchi' (Manage blocks) settings page. The browser address bar shows the URL <https://www.facebook.com/settings?tab=blocking>. The page title is '(20) Gestisci i blocchi'. The user's name is 'Domenico'. The left sidebar contains navigation options: Generali, Protezione, Privacy, Diario e aggiunta di..., Blocco (selected), Lingua, Notifiche, Per cellulare, Post pubblici, App, Inserzioni, Pagamenti, Riepilogo segnalazi..., and Video. The main content area is titled 'Gestisci i blocchi' and contains several sections:

- Lista limitata:** Quando aggiungi un amico alla tua lista Con restrizioni, questa persona non vedrà su Facebook i contenuti che condividi impostando la privacy su "Amici". Vedrà soltanto i contenuti che pubblichi con la privacy impostata su "Tutti", sul diario di un amico in comune o quelli in cui lo taggano. Facebook non invierà una notifica alle persone che aggiungi alla tua lista Con restrizioni. [Scopri di più](#) [Modifica lista](#)
- Blocco di utenti:** Quando blocchi una persona, questa non potrà più vedere le cose che pubblichi sul tuo diario, taggarti, invitarti agli eventi o ai gruppi, avviare una conversazione con te o aggiungerti agli amici. Nota: questa limitazione non viene applicata ad applicazioni, giochi o gruppi che condividete. **Blocca questi utenti** **Blocca**
Non hai aggiunto nessuno all'elenco utenti bloccati.
- Blocco dei messaggi:** Se blocchi i messaggi e i video di qualcuno qui, questa persona non potrà contattarti neanche nell'applicazione Messenger. A meno che non blocchi il profilo di qualcuno, questa persona potrebbe pubblicare nel tuo profilo, taggarti e commentare i tuoi post o i commenti. [Scopri di più](#). **Blocca i messaggi di:**
- Blocco di inviti alle applicazioni:** Una volta bloccati gli inviti relativi alle applicazioni da parte di qualcuno, ignorerai automaticamente tutte le richieste per applicazioni che ti verranno inviate in futuro da tale persona. Per bloccare gli inviti da parte di un amico specifico, clicca sul link "Ignora tutti gli inviti da questo/a amico/a" sotto l'ultima richiesta ricevuta da quella persona. **Blocca gli inviti da**
- Blocco di inviti agli eventi:** Una volta bloccati gli inviti di qualcuno, ignorerai automaticamente le richieste di partecipazione a eventi futuri da parte di tale persona.

At the bottom right, there is a 'Chat (1)' notification and a settings icon.

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.

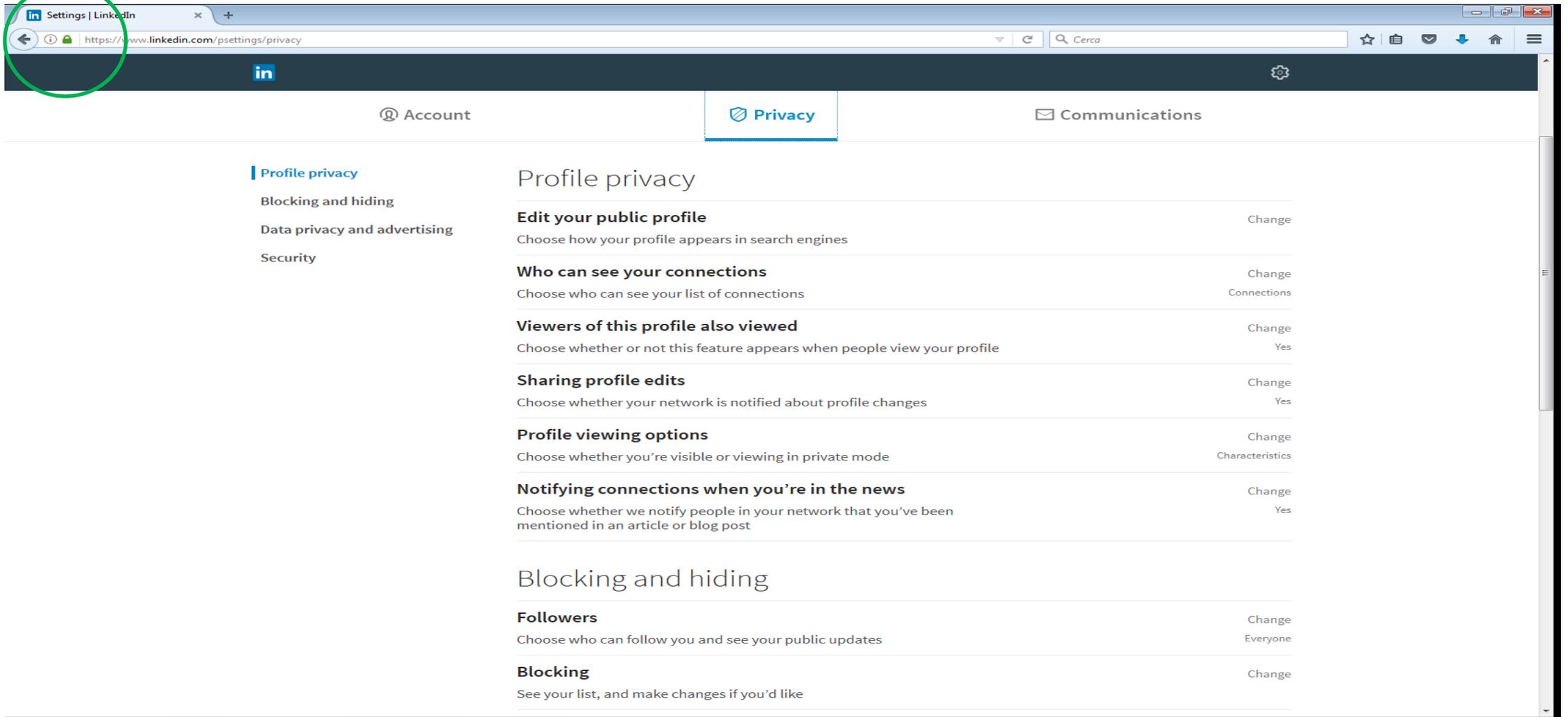
Comportamenti degli utenti

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

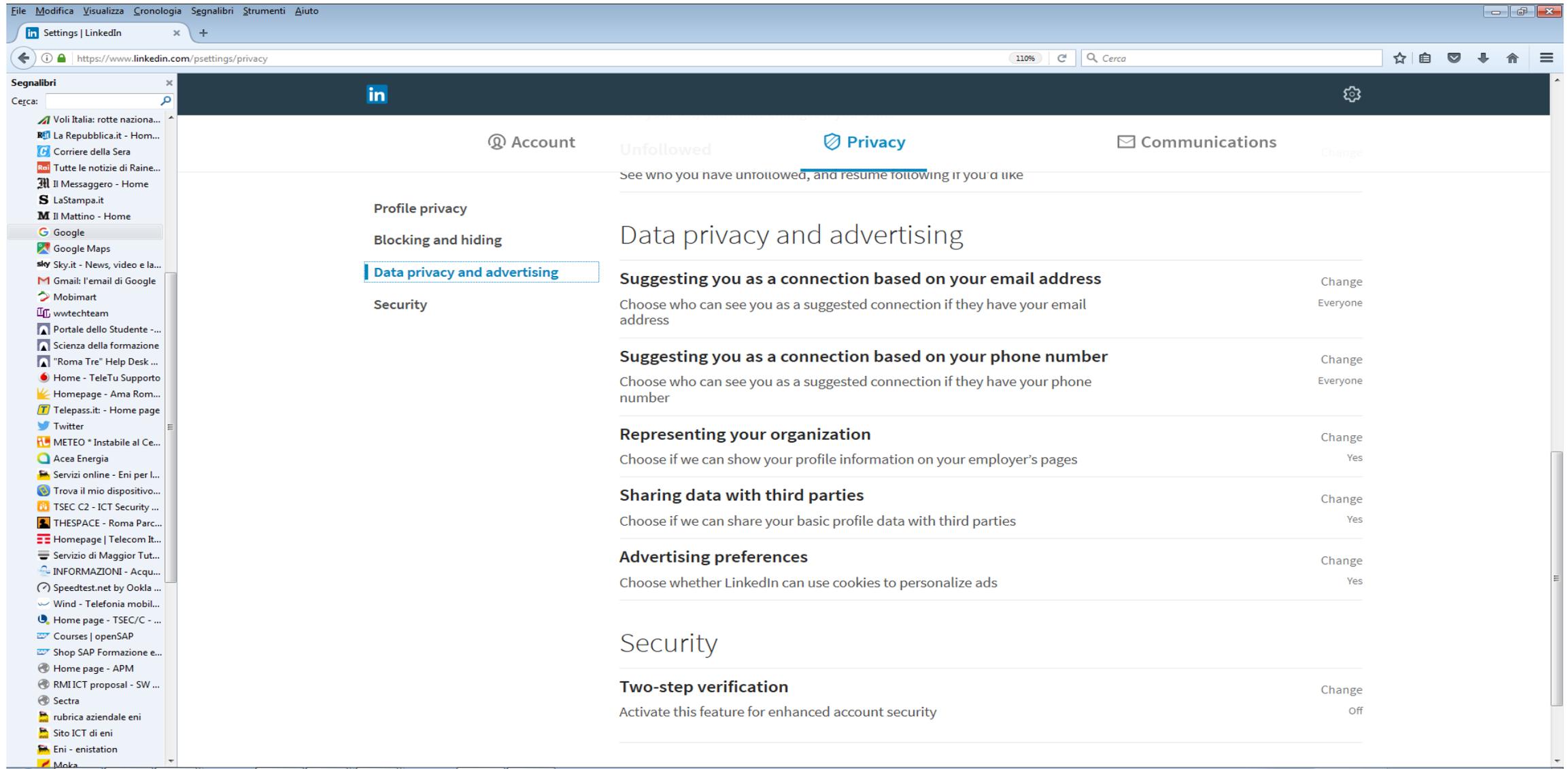
Sito sicuro



The screenshot shows the LinkedIn Privacy Settings page. A green circle highlights the address bar, which contains the URL <https://www.linkedin.com/psettings/privacy>. A green arrow points from the text 'Sito sicuro' to the lock icon in the address bar. The page is divided into three main sections: Account, Privacy (selected), and Communications. The Privacy section is further divided into Profile privacy, Blocking and hiding, and Security. The Profile privacy section includes settings for Edit your public profile, Who can see your connections, Viewers of this profile also viewed, Sharing profile edits, Profile viewing options, and Notifying connections when you're in the news. The Blocking and hiding section includes settings for Followers and Blocking.

Section	Setting	Description	Action
Profile privacy	Edit your public profile	Choose how your profile appears in search engines	Change
	Who can see your connections	Choose who can see your list of connections	Change Connections
	Viewers of this profile also viewed	Choose whether or not this feature appears when people view your profile	Change Yes
	Sharing profile edits	Choose whether your network is notified about profile changes	Change Yes
	Profile viewing options	Choose whether you're visible or viewing in private mode	Change Characteristics
	Notifying connections when you're in the news	Choose whether we notify people in your network that you've been mentioned in an article or blog post	Change Yes
Blocking and hiding	Followers	Choose who can follow you and see your public updates	Change Everyone
	Blocking	See your list, and make changes if you'd like	Change

Comportamenti degli utenti



The screenshot shows the LinkedIn Privacy Settings page. The browser address bar displays 'https://www.linkedin.com/psettings/privacy'. The page is divided into three main sections: 'Account', 'Privacy', and 'Communications'. The 'Privacy' section is active and contains several settings:

- Profile privacy**
- Blocking and hiding**
- Data privacy and advertising** (highlighted):
 - Suggesting you as a connection based on your email address**: Set to 'Everyone'.
 - Suggesting you as a connection based on your phone number**: Set to 'Everyone'.
 - Representing your organization**: Set to 'Yes'.
 - Sharing data with third parties**: Set to 'Yes'.
 - Advertising preferences**: Set to 'Yes'.
- Security**:
 - Two-step verification**: Set to 'Off'.

The left sidebar shows a list of bookmarks, including 'Voli Italia: rotte naziona...', 'La Repubblica.it - Hom...', 'Corriere della Sera', 'Tutte le notizie di Raine...', 'Il Messaggero - Home', 'LaStampa.it', 'Il Mattino - Home', 'Google', 'Google Maps', 'Sky.it - News, video e la...', 'Gmail: l'email di Google', 'Mobimart', 'wwtchteam', 'Portale dello Studente - ...', 'Scienza della formazione', '"Roma Tre" Help Desk ...', 'Home - TeleTu Supporto', 'Homepage - Ama Rom...', 'Telepass.it - Home page', 'Twitter', 'METEO * Instabile al Ce...', 'Acea Energia', 'Servizi online - Eni per l...', 'Trova il mio dispositivo...', 'TSEC C2 - ICT Security ...', 'THESPACE - Roma Parc...', 'Homepage | Telecom It...', 'Servizio di Maggior Tut...', 'INFORMAZIONI - Acqu...', 'Speedtest.net by Ookla ...', 'Wind - Telefonia mobil...', 'Home page - TSEC/C - ...', 'Courses | openSAP', 'Shop SAP Formazione e...', 'Home page - APM', 'RMI ICT proposal - SW ...', 'Sectra', 'rubrica aziendale eni', 'Sito ICT di eni', 'Eni - enistation', and 'Moka'.

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 generare 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.

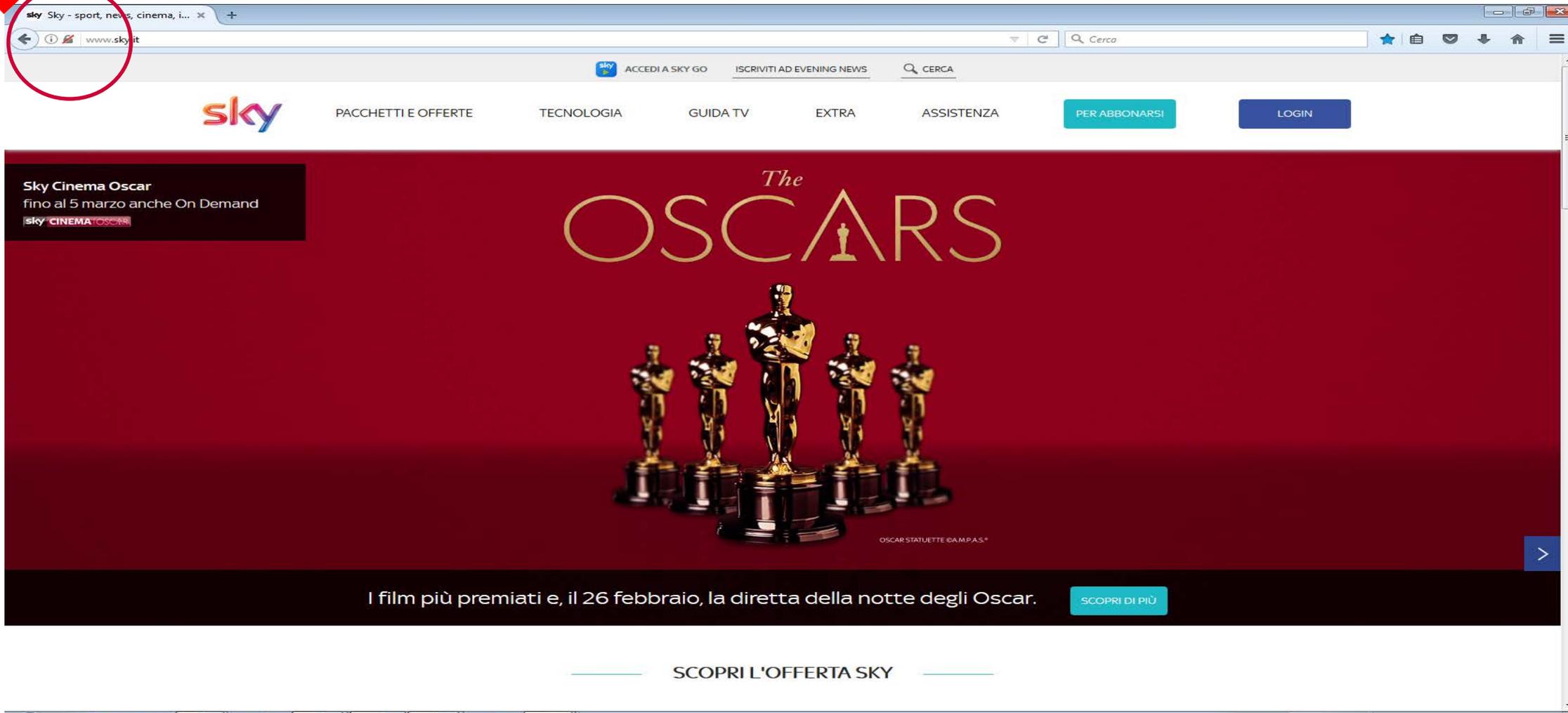
DURANTE IL VIAGGIO

- 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

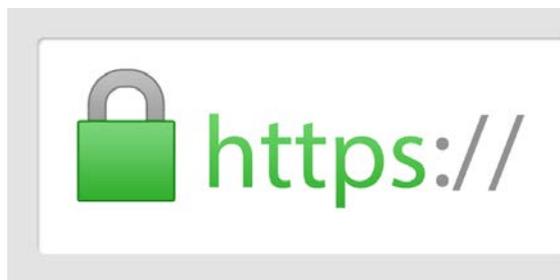


Comportamenti degli utenti

Sito non sicuro



Comportamenti degli utenti



Informazioni pagina - https://upload.wikimedia.org/wikipedia/commons/e/e5/HTTPS_icon.png

Generale Media Permessi Sicurezza

Identità sito web

Sito web: **upload.wikimedia.org**
Proprietario: **Non sono disponibili informazioni sul proprietario di questo sito web.**
Verificata da: **DigiCert Inc**

[Visualizza certificato](#)

Privacy e cronologia

Questo sito è già stato visitato prima di oggi?	No	
Questo sito web sta memorizzando informazioni (cookie) sul computer?	Sì	Mostra cookie
Esistono password memorizzate per questo sito web?	No	Mostra password

Dettagli tecnici

Connessione crittata (TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, chiavi a 256 bit, TLS 1.2)

La pagina visualizzata è stata crittata prima della trasmissione via Internet.

La crittazione rende difficile osservare le informazioni scambiate tra computer a persone non autorizzate. È quindi improbabile che qualcuno sia riuscito a leggere il contenuto di questa pagina durante il transito attraverso la rete.

[Guida](#)

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 prelievi 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.