



# **SICUREZZA DELLA RETE INTERNET**

**Giovanni Parascandolo**

Roma, 25 novembre 2017

# SURFACE WEB

Wikipedia Google Bing

# DEEP WEB

Academic Information  
Medical Records  
Legal Documents  
Scientific Reports  
Subscription Information

Multilingual Databases  
Conference Proceedings  
Government Resources  
Competitor Websites  
Organization-specific  
Repositories

# DARK WEB

Illegal Information

Drug Trafficking sites

TOR-Encrypted sites

Private Communications

AUG  
2017

# GLOBAL DIGITAL SNAPSHOT

THE LATEST NUMBERS FOR INTERNET, SOCIAL MEDIA, AND MOBILE USAGE AROUND THE WORLD

TOTAL  
POPULATION



we  
are  
social

**7.524**  
BILLION

URBANISATION:

**54%**

INTERNET  
USERS



**3.819**  
BILLION

PENETRATION:

**51%**

ACTIVE SOCIAL  
MEDIA USERS



we  
are  
social

**3.028**  
BILLION

PENETRATION:

**40%**

UNIQUE  
MOBILE USERS

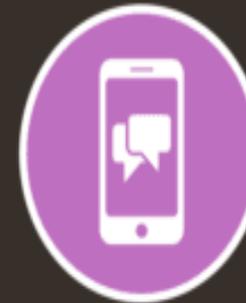


**5.052**  
BILLION

PENETRATION:

**67%**

ACTIVE MOBILE  
SOCIAL USERS



**2.780**  
BILLION

PENETRATION:

**37%**

**SOURCES:** POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; INTERNETLIVESTATS; CIA WORLD FACTBOOK; FACEBOOK; NATIONAL REGULATORY AUTHORITIES; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; LIVEINTERNET.RU; KAKAO; NAVER; NIKI AGHAEI; CAFEBAZAAR.IR; SIMILARWEB; DING; EXTRAPOLATION OF TNS DATA; MOBILE: GSMA INTELLIGENCE; EXTRAPOLATION OF EMARKETER AND ERICSSON DATA.

 **Hootsuite™** we  
are  
social

Fonte: [www.wearesocial.com](http://www.wearesocial.com) – report "digital 2017"

JAN  
2017

# DIGITAL IN ITALY

A SNAPSHOT OF THE COUNTRY'S KEY DIGITAL STATISTICAL INDICATORS



TOTAL  
POPULATION



we  
are  
social

**59.80**  
MILLION

URBANISATION:

**69%**

INTERNET  
USERS



**39.21**  
MILLION

PENETRATION:

**66%**

ACTIVE SOCIAL  
MEDIA USERS



we  
are  
social

**31.00**  
MILLION

PENETRATION:

**52%**

UNIQUE  
MOBILE USERS



**50.77**  
MILLION

PENETRATION:

**85%**

ACTIVE MOBILE  
SOCIAL USERS



**28.00**  
MILLION

PENETRATION:

**47%**

3

**SOURCES:** POPULATION: UNITED NATIONS; U.S. CENSUS BUREAU; INTERNET: INTERNETWORLDSTATS; ITU; INTERNETLIVESTATS; CIA WORLD FACTBOOK; FACEBOOK; NATIONAL REGULATORY AUTHORITIES; SOCIAL MEDIA AND MOBILE SOCIAL MEDIA: FACEBOOK; TENCENT; VKONTAKTE; LIVEINTERNET.RU; KAKAO; NAVER; NIKI AGHAEI; CAFEBAZAAR.IR; SIMILARWEB; DING; EXTRAPOLATION OF TNS DATA; MOBILE: GSMA INTELLIGENCE; EXTRAPOLATION OF EMARKETER AND ERICSSON DATA.



Hootsuite™

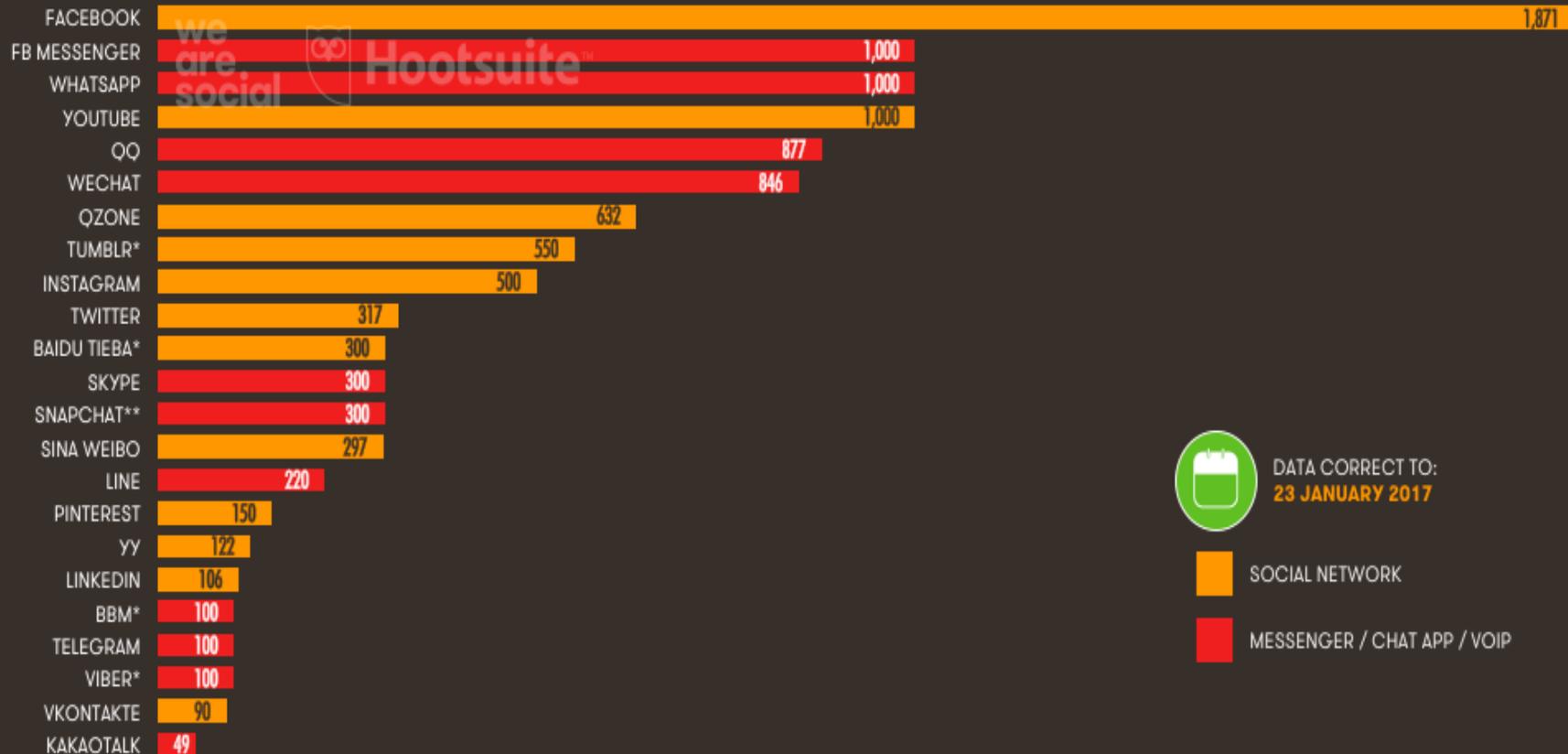
we  
are  
social

Fonte: [www.wearesocial.com](http://www.wearesocial.com) – report "digital 2017"

JAN  
2017

# ACTIVE USERS OF KEY GLOBAL SOCIAL PLATFORMS

BASED ON THE MOST RECENTLY PUBLISHED MONTHLY ACTIVE USER ACCOUNTS FOR EACH PLATFORM, IN MILLIONS



DATA CORRECT TO:  
23 JANUARY 2017



SOCIAL NETWORK



MESSENGER / CHAT APP / VOIP

48

SOURCES: WE ARE SOCIAL ANALYSIS; LATEST COMPANY EARNINGS RELEASES, PRESS RELEASES OR MEDIA STATEMENTS; REPORTS IN REPUTABLE MEDIA; ALL AS OF JANUARY 2017.  
\*NOTE: PLATFORMS IDENTIFIED BY AN ASTERISK (\*) HAVE NOT PUBLISHED UPDATED USER FIGURES IN THE PAST 12 MONTHS, SO FIGURES MAY BE OUT OF DATE AND LESS RELIABLE.  
\*\*NOTE: SNAPCHAT DOES NOT PUBLISH MONTHLY ACTIVE USER DATA. THE FIGURE USED HERE WAS REPORTED BY BUSINESS INSIDER IN JUNE 2016, BASED ON DAILY ACTIVE USERS.



Fonte: [www.wearesocial.com](http://www.wearesocial.com) – report "digital 2017"

# Il Phishing 1/4

Tecnica che utilizza finte *e-mail* e falsi siti *web* per sottrarre dati personali, credenziali di accesso, *user-id* e *password*, coordinate bancarie etc.

Spesso utilizzano *mail* di spam anche se a volte utilizzano tecniche dette di «*cross site scripting XSS*» per installare software malevolo o dirottare gli utenti;

Come funziona il *phishing*:



PHISHER



TITOLARE C/C

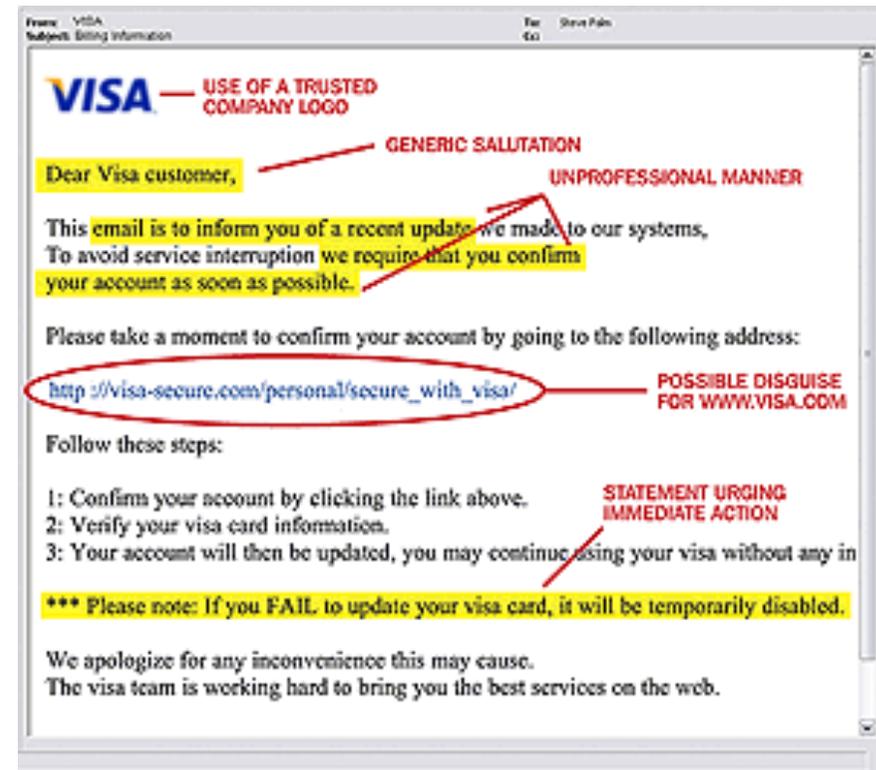
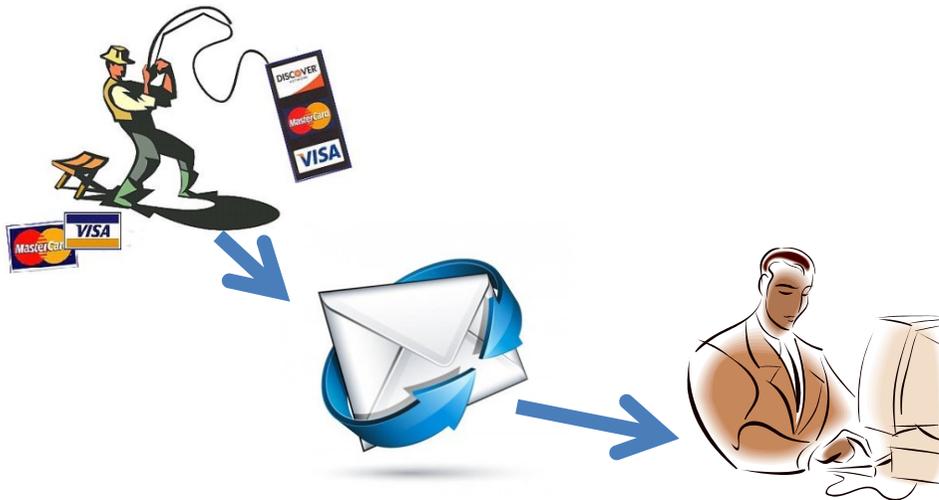


ASPIRANTE COLLABORATORE

# Il Phishing 2/4

Come funziona il *phishing*:

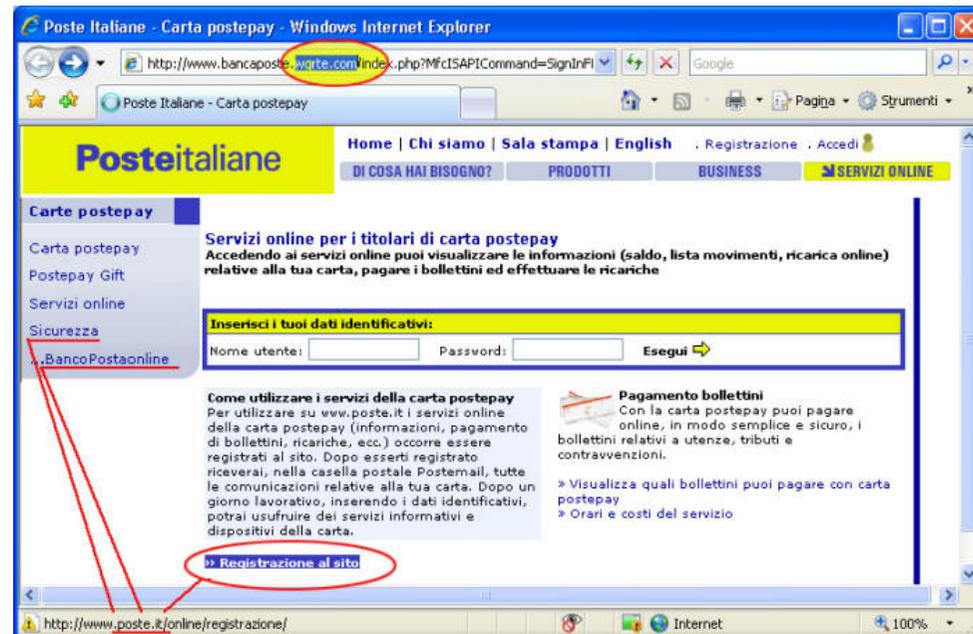
1. Il phisher invia una mail fraudolenta ad un utente invitandolo a collegarsi al sito della propria banca (oppure ad un *social network*) oppure ad aprire un allegato.



# Il Phishing 3/4

Come funziona il *phishing*:

2. l'utente viene dirottato verso un finto sito di un istituto di credito o *social network*.... ed inserisce le proprie credenziali;



# Il Phishing 4/4

Come funziona il *phishing*:

3. il *phisher* non può effettuare bonifici sul suo conto corrente, altrimenti sarebbe subito smascherato. Invia quindi una mail contenente una falsa offerta di lavoro a domicilio ad un soggetto terzo... chi risponde non dovrà far altro che indicare il proprio IBAN ed essere disponibile a ricevere dei bonifici.

Parte di quanto riceve lo dovrà inviare a soggetti terzi attraverso agenzie di *money transfer*, e lui si terrà una piccola percentuale a titolo di commissione



# I Ransomware

The image shows two overlapping screenshots. The top one is from the Guardia di Finanza website, featuring the Italian flag and the text "Guardia di Finanza insieme per la legalità". It contains a warning message in Italian: "Attenzione!!! È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violazione delle leggi della Repubblica Italiana! È stata fissata una seguente violazione: Dal tuo indirizzo IP '...' era eseguito un accesso alle web-pagine contenenti la pornografia, la pornografia minorile, zoofilia, nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile. Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recredito terroristico. Il blocco di computer serve per troncane l'attività illegale dalla parte tua." Below this, it lists two payment options: 1) using Ukash and 2) using Paysafecard. The bottom screenshot is a ransom note from CTB-Locker with a black background and yellow text. It reads: "I tuoi dati personali sono criptati da CTB-Locker". It states that files are encrypted and provides a 96-hour deadline for payment. A countdown timer shows 95:59:43. Buttons for "Esamina" and "Avanti >>" are visible at the bottom.

## Crime pays very well: Cryptolocker grosses up to \$30 million in ransom

By [Dave Jeffers](#), BrandPost

Dec 20, 2013 12:45 PM

No wonder [street crime is down](#). If you want to make a dishonest living, cybercrime is the place to be. According to a [Dell SecureWorks report](#) by Keith Jarvis, the creators of the notorious CryptoLocker ransomware virus may have made as much as \$30 million in a mere 100 days.

That's a lot more than you'd earn stealing people's iPhones --and you're far less likely to get caught. (It's also a lot more than you'd get doing honest work.)

# I Social Network



I social network hanno cambiato il concetto di amicizia del XXI secolo... ci sono persone che hanno migliaia di amici...

Più «amici» si hanno e più si è esposti al problema del furto di identità online

Ma cos'è un amico?

## Numero di Dunbar

Da Wikipedia, l'enciclopedia libera.

Il **numero di Dunbar** è una quantificazione numerica del **limite cognitivo teorico** che concerne il numero di persone con cui un **individuo** è in grado di mantenere **relazioni sociali** stabili, ossia relazioni nelle quali un individuo conosce l'**identità** di ciascuna persona e come queste persone si **relazionano con ognuna delle altre**.<sup>[1][2][3][4][5][6]</sup>

Le stime sul valore del numero di Dunbar, in realtà, oscillano tra 100 e 250, ma l'approssimazione adoperata di solito è 150.

# 1997



partendo dalla teoria dei "6 gradi di separazione",  
nasce il primo social network



- oltre 200 social network
- circa 40 portali specializzati in incontri

## I social media possono essere suddivisi in:



- ✓ *profile-based*
- ✓ *content-based*
- ✓ *entertainment*
- ✓ *business*
- ✓ *etnici/comunità*
- ✓ *blog-based*
- ✓ *micro-blogging*
- ✓ *tematici*
- ✓ *mobile*





**Social network, un'opportunità per le aziende....**



**.... ma anche per le organizzazioni criminali**

**Attenzione a ciò che si pubblica....**



**...ed alla propria reputazione ...**





**L'immaterialità della “piazza virtuale”  
amplifica le disinibizioni, le volgarità e  
le condotte illecite**



**sexting**



**stalking**



**cyberbullismo**



**diffamazione**

**Libero** - 15 dicembre 2016

La statistica di una società di allarmi

# Tre ladri su quattro usano i social per scegliere le case da razzare

I banditi controllano su Facebook, Instagram e Twitter la disponibilità economica e i movimenti delle potenziali vittime. Ecco quali regole seguire per tenerli alla larga

di GIANLUCA VENEZIANI

■ ■ ■ Oggi anche il Kevin di "Mamma ho perso l'aereo", anziché manichini, trappole e voci di film registrati per scacciare via i ladri, prenderebbe le adeguate contromisure sui social network. I ladri non sono più quella copia di scalcagnati malviventi che attentano a casa McCallister, ma si sono aggiornati a livello tecnologico e utilizzano Facebook, Twitter o Instagram per portare a termine i loro furti: rubano informazioni alle vittime per poi rubare oggetti nelle loro case.

Come rende noto Verisure, società leader in Europa nel mercato degli allarmi, addirittura il 75% dei ladri - vale a dire tre su quattro - si avvale dei social per identificare le potenziali vittime, capire cosa possiedono, dove vivono e quanto tempo trascorrono

scaccia-ladri. Ecco qua alcuni consigli utili. In primis, è bene non condividere sui social informazioni personali come la via di casa, il posto di lavoro e il proprio numero di telefono. In secondo luogo, è preferibile evitare di postare in tempo reale su Facebook, Twitter o Instagram le foto dei propri viaggi: il che non vuol dire autocensurare per paura ogni immagine di vacanza, ma pubblicarla in modo intelligente nel momento in cui si torna a casa (magari varrà qualche "like" in meno postarla l'8 gennaio, ma si guadagna in tranquillità). In terzo luogo, sarebbe bene disattivare sui social la geolocalizzazione, che spesso viene inserita automaticamente. Così come impostare la privacy in modo che solo gli amici possano vedere

il gioco facile per svaligiare le abitazioni (in un rovesciamento simbolico inquietante per cui sottraggono cose anziché portare doni, come fanno le persone perbene). Altri dati Verisure relativi al 2015 dimostrano infatti che nel mese di dicembre i furti raddoppiano rispetto alla media dell'anno, con una percentuale del 14% sul totale annuo rispetto al 7-8% degli altri mesi. E questo in un contesto in cui la paura di essere derubati cresce insieme alla sensazione generale di pericolo. Un sondaggio condotto dall'Istituto Sondea nel 2016 conferma che un italiano su due teme un'intrusione in casa e ben 8 italiani su 10 crederanno un amico o un familiare che ha subi-

VareseNews

VareseNews

<http://www.varesenews.it>

## Occhio al post: ladri in agguato su Facebook

Data: 18 agosto 2016

L'ultima frontiera dei furti in appartamento durante la stagione estiva sono i social network. «Sono sempre più i ladri, stando ai dati divulgati dalle Forze dell'Ordine, che scelgono di monitorare gli spostamenti delle future vittime su Facebook, onde agire indisturbati sapendo di trovare con certezza l'abitazione libera».

Lo dichiara l'avvocato Patrizia Polliotto, Fondatore e Presidente del Comitato Regionale del Piemonte dell'Unione Nazionale Consumatori, dal 1955 a oggi la più antica e autorevole associazione consumeristica italiana.

La raccomandazione è quella, per i consumatori, di non scrivere o pubblicare post sui social network, in cui si danno informazioni di ogni genere legate ai propri spostamenti, stando di rendere noto se si è fuori casa e per quanto tempo, se in vacanza.

tenere sempre gli occhi  
le chiavi



## **POSSIBILI RIMEDI**

**Il primo accorgimento da adottare è leggere accuratamente il codice di condotta e le regole applicate sul trattamento dei dati da parte del social network...**

**... sarà poi necessario:**

## **POSSIBILI RIMEDI**

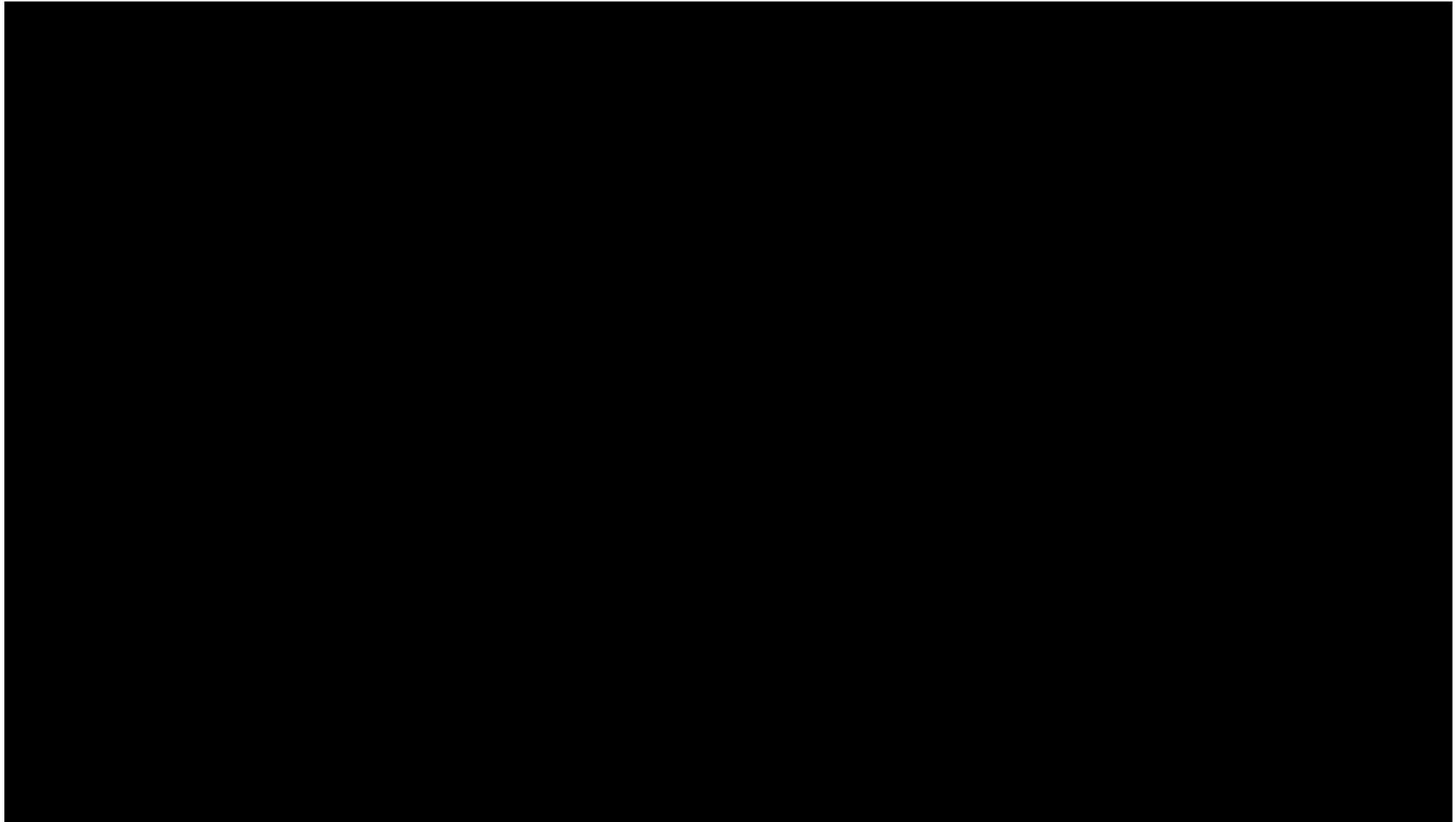
- ✓ **utilizzare di password “robuste”**
- ✓ **porre attenzione alle impostazioni della privacy del proprio profilo**
- ✓ **verificare i dettagli delle fotografie pubblicate (EXIF)**
- ✓ **evitare l’uso di dati identificativi completi**
- ✓ **considerare cosa viene pubblicato e gli effetti che potrebbe assumere nel tempo**

**... sarà poi necessario:**

## **POSSIBILI RIMEDI**

- ✓ **riflettere sul fatto che di ogni contenuto che si immette in Rete, se ne perde il controllo, rendendolo di fatto “immortale”**
- ✓ **non sottovalutare la rilevanza professionale del proprio profilo personale**
- ✓ **pubblicare informazioni attinenti alle vacanze o viaggi di lavoro soltanto a posteriori**
- ✓ **mantenere il proprio PC ed antivirus aggiornati**

**... e per concludere...**



*"If you are not paying for it, you're  
not the customer;  
you're the product being sold."*

**Grazie  
per l'attenzione**