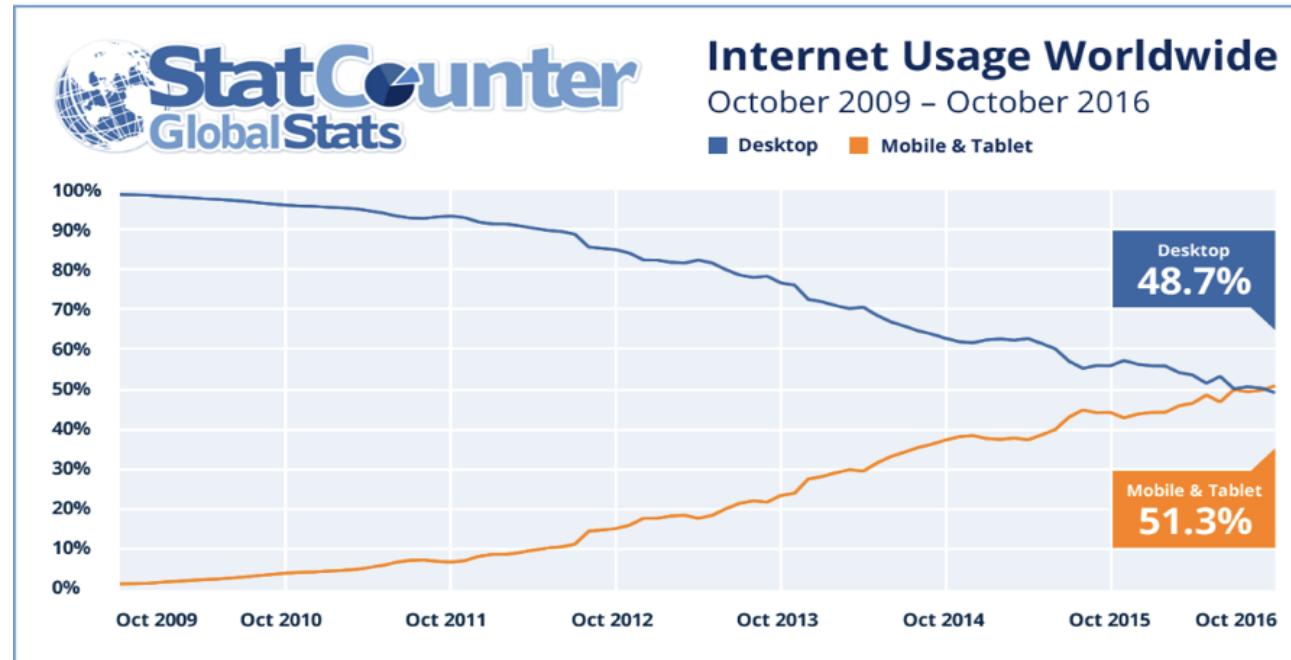




Sicurezza digitale

Smartphone e sicurezza



Da quando (nel 2016) il traffico mobile ha superato quello fisso, il **cybercrime** ha aumentato sempre più la propria attenzione verso i dispositivi mobili.

Android oggi rappresenta circa l'80% del mondo mobile (con Apple iOS che ha il restante 20%), quindi è ovviamente il “bersaglio grosso” più facile da attaccare. Per i cyber criminali, sono diventati una potenziale miniera d'oro di **dati personali**

Attualmente il metodo più sfruttato dal malware per infiltrarsi in un dispositivo mobile è tramite il download di un'**app malevola** che non sia stata sottoposta ad adeguati controlli.

Quindi è **estremamente importante** mantenere sempre aggiornati i propri **smartphone**. Purtroppo, questa scelta non sempre è possibile per l'utente finale, a causa della complessità della filiera di Android. Questa richiede fino a cinque fasi prima che l'aggiornamento arrivi sullo smartphone dell'utente:

- Android (Google) realizza l'aggiornamento.
- Android invia l'aggiornamento ai produttori di processori (per es. Qualcomm) che lo devono adattare ai propri hardware specifici.
- Poi viene inviato ai produttori di smartphone (Samsung, LG, Huawei, ecc.) che personalizzano la nuova release.
- Successivamente passa ai provider che vendono propri dispositivi mobili ai clienti, e che possono apportare le proprie modifiche al software.

Solo a questo punto la nuova versione del sistema operativo viene rilasciata al pubblico.

Nel sistema Apple iOS la filiera è invece estremamente corta e verticale: da Apple gli aggiornamenti arrivano direttamente all'utente (con un solo passaggio) e interessano un numero di modelli estremamente limitato. Questo fa sì che oggi, nel 2022, anche uno smartphone nato diversi anni fa, come iPhone 7, sia ancora supportato a distanza di 6 anni.

Connessioni in chiaro e crittografate

- Connessioni “normali” e connessioni sicure

- [http://](#) → traffico in chiaro!
- [https://](#) → traffico crittografato!



Password

- Quindi...
- utente e password SOLO con https
- verificare SEMPRE il lucchetto (certificato valido)



Una password FORTE (strong) è una password difficile da indovinare. Le password FORTI hanno queste caratteristiche:

LUNGHEZZA: più sono lunghe più sono SICURE. Ottimale almeno 8 caratteri

VARIETA': la password dovrebbe contenere almeno un carattere maiuscolo, almeno un numero e/o simboli.

INSOLITA: la password non dovrebbe appartenere ad un dizionario e non essere un nome proprio



Tempo stimato per «forzare» una password ben costruita

Estimated time to brute force psw crack				
@ 100.000 per second				
passw	26	36	52	96
length	non-case	alphanum.	upper/lower	all print.
4	<1min	<1min	1 min	13 min
5	<1min	10 min	1hr	22 hrs
6	50 min	6 hr	2 days	3 mo
7	22 hr	9 days	4 mo	20 yrs
8	24 days	10 mo	17 yrs	2287 yrs
9	21 mo	33 yrs	881 yrs	219000 yrs
10	45 yrs	1159 yrs	45838 yrs	21 myrs

<https://www.google.com/preferences>

Controllo contenuti (sesso e violenza)