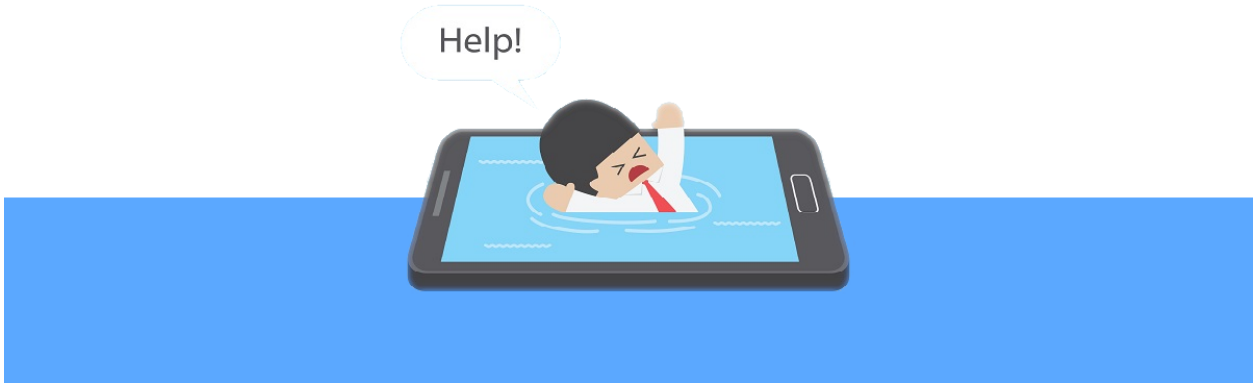
UNIVERSITÀ
DI SIENA
1240

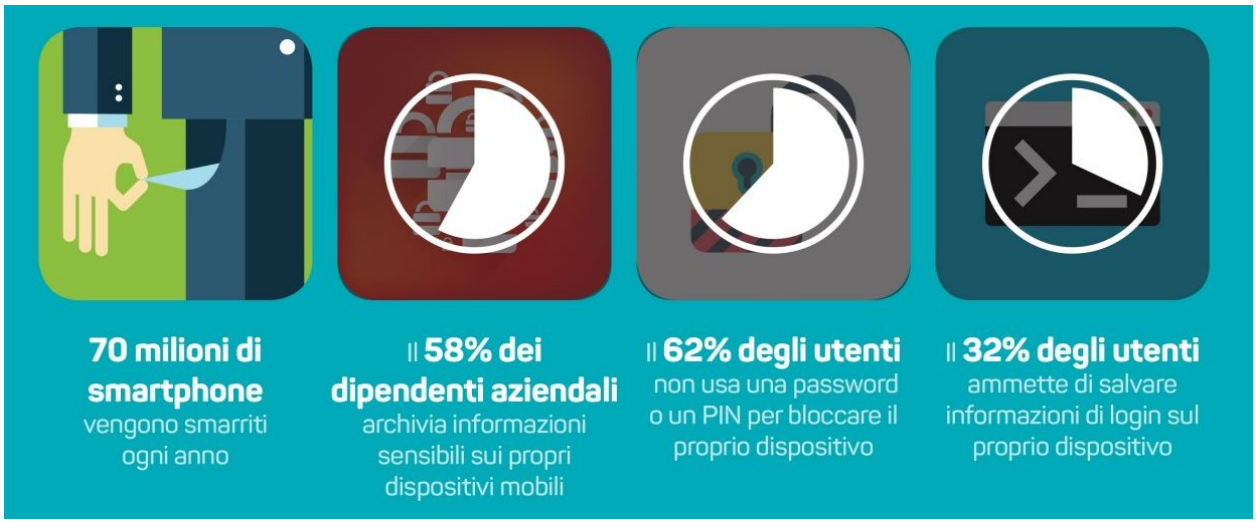
UniSIcuri in Rete - Occhio allo smartphone!

Gennaio 2021



Le minacce ai nostri smartphone

I dati ci dicono che **l'Italia è uno dei Paesi con maggiore presenza di *smartphone* tra la popolazione.** Il "telefonino", che ormai assomiglia sempre di più a un PC vero e proprio che a un telefono, è diventato parte integrante della nostra *onlife* quotidiana: lo usiamo per restare in contatto con amici, colleghi e parenti, per svago, per lavorare, per informarsi.



La memoria del nostro *smartphone* è quotidianamente infarcita di dati che riguardano la nostra vita, dalle e-mail ai documenti di lavoro, dalle foto alle chat personali: è quindi essenziale proteggere queste informazioni da utilizzi indesiderati, oltre a tutta una serie di attacchi specifici del mondo "mobile", come il *sim swapping*.

👉 Il 93% delle aziende ha dispositivi mobili connessi alla propria Rete

È opportuno considerare anche quanto **ormai il nostro smartphone sia diventato elemento essenziali per accedere a servizi bancari e finanziari**, come ad esempio l'invio di OTP via SMS o l'utilizzo di strumenti di autenticazione biometrica (volto, impronta digitale) per accedere all'*home banking*.

👉 Il 58% dei dipendenti aziendali archivia informazioni sensibili sui propri dispositivi mobili

---

Proprio per questa caratteristica **molti gruppi di cybercriminali hanno preso di mira le piattaforme mobili, realizzando strumenti malevoli in grado di rubare le credenziali di accesso** alle piattaforme di *home banking*. Questa tipologia di attacco, chiamata "pharming", è in forte crescita e secondo alcune autorevoli stime **rappresenta quasi il 50% di tutte le minacce cybernetiche**[1] individuate in Europa.

Giusto per chiarire, nella categoria dei dispositivi mobili rientrando a pieno titolo anche i tablet. Spesso considerati dispositivi ibridi tra uno smartphone e un PC portatile, il tablet - *soprattutto se utilizzato come strumento di lavoro* - è un dispositivo mobile con gli stessi elementi di criticità di uno smartphone.

[1] *I malware per furto di credenziali: gli scenari in Europa*, *Data Manager Online*

I principali rischi di sicurezza

Ricapitolando, il nostro *smartphone* può essere colpito da queste tipologie di attacco:

- ***Sim Swapping*** - Utilizzando alcune informazioni personali, insieme all'ICCID della scheda SIM, un attaccante può ottenere una copia della nostra SIM card ed utilizzarla per leggere i nostri messaggi e per ricevere le chiavi OTP dell'home banking;
- ***Pharming*** - Come già anticipato, attraverso l'utilizzo di applicazioni malevole installate sullo smartphone ("*malware*"), vengono rubate informazioni personali e dati di accesso ai servizi on-line;
- ***Smishing*** - Phishing via SMS, inviando messaggi fraudolenti per indurre l'utente a visitare un certo sito web e inserire informazioni personali;

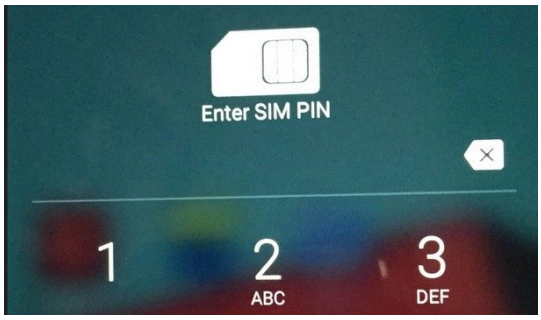
A cui si aggiungono tutte le minacce comuni ai dispositivi informatici, tra cui il **furto/ smarrimento** del dispositivo: la perdita di possesso fisica dello *smartphone* può esporre i dati in esso contenuti a utilizzi indebiti, ad esempio sfruttando le fotografie in esso contenute per la creazioni di profili social fasulli (furto d'identità), attivazione di servizi a nostra insaputa, vendita sul mercato nero delle credenziali e dei documenti...

👉 Il 65% dei dipendenti utilizza i propri dispositivi mobili per l'accesso alla posta elettronica aziendale

Compreso, ovviamente, l'utilizzo dei dispositivi mobili (smartphone/tablet) connessi alle reti aziendali per sferrare attacchi contro di esse.

Prevenzione

Per **difendersi dalle minacce *cyber* ai nostri dispositivi mobili** dobbiamo attuare una serie di azioni di prevenzione, per evitare incidenti e per essere eventualmente pronti e il più possibile tutelati in caso di problemi.



➔ **PIN sulla scheda SIM** - Impostare la richiesta del codice PIN per sbloccare la scheda SIM a ogni accensione dello smartphone. È sempre possibile modificare il codice PIN in modo che sia più facile da ricordare (evitate sempre l'uso di '0000'). In caso di smarrimento o di furto, il PIN sulla scheda eviterà, insieme ad altre misure di protezione, utilizzi indebiti del vostro numero di telefono.

➔ **PIN o segno di blocco** - Impostare l'inserimento di un PIN numerico o di un segno di sblocco per l'accesso alle funzioni dello smartphone dopo un periodo di inutilizzo (es. 5 minuti). Questa misura impedirà, in caso di furto o smarrimento, l'utilizzo indebito dello smartphone.

➔ **Cifratura del dispositivo e della scheda SD** - Gli smartphone più aggiornati hanno già la cifratura della memoria interna abilitata di

default: assicuratevi che sia attiva. Inoltre, per maggiore sicurezza, anche la scheda di memoria miniSD dovrebbe essere cifrata: in caso di furto o smarrimento, un malintenzionato potrebbe facilmente accedere ai dati dentro la scheda di memoria...

➔ **Installare solo APP da fonti affidabili** - Evitate l'installazione di app da fonti o produttori sconosciuti. Spesso il malware si nasconde all'interno di giochi o di app craccate, quindi chiedetevi sempre se vale la pena...

➔ **Attivate il backup automatico** - I dispositivi Android permettono, previa autenticazione con il proprio account di Google, di impostare il backup automatico dei dati: una funzione utile in caso di furto, danneggiamento o smarrimento del dispositivo, perché permette di recuperare tutto, rubrica compresa, in pochi passaggi. Maggiori informazioni qui: https://support.google.com/android/answer/2819582

➔ **Attivate la localizzazione del dispositivo** - Sempre Google offre, per i dispositivi Android, la funzione "*Trova il tuo telefono*" (https://myaccount.google.com/find-your-phone?pli=1). *Assicuratevi che funzioni prima di doverla utilizzare... per necessità!*

➔ **Effettuare sempre gli aggiornamenti** - Mantenete sempre lo smartphone aggiornato alle ultime versioni dei software, che correggono

eventuali problematiche e falle di sicurezza. Se avete uno smartphone fuori assistenza, che non riceve più aggiornamenti, meditate seriamente di passare a un modello più aggiornato.

➔ **Affidarsi a produttori noti** - Smartphone prodotti da piccole aziende sconosciute non europee, anche se più economici, potrebbero essere non conformi alle normative di sicurezza, affetti da vulnerabilità o non ricevere adeguati aggiornamenti di sicurezza[2]. Così come non risparmieremmo sulla serratura di casa, conviene investire qualche euro in più quando si parla di proteggere la nostra identità e dati personali.

È sempre opportuno **evitare di prestare a terzi il proprio *smartphone*** e di **utilizzare il medesimo dispositivo per lavoro e per svago** o motivi personali.

Ricordiamo inoltre che **non è consentito il salvataggio di documenti istituzionali riservati o contenenti informazioni personali o altri dati particolari su dispositivi personali** o comunque non adeguatamente protetti secondo quanto previsto dalla normativa vigente.

In caso di furto o smarrimento...

La prima cosa da fare, in questi casi, è procedere immediatamente con la **modifica di tutte le credenziali dei servizi** che avevamo attivato sullo smartphone: dalla posta elettronica all'*home banking*, dai *social network* a eventuali *chat*, è buona norma procedere immediatamente al cambio di tutte le password di accesso.

👉 Possiamo effettuare una verifica delle attività effettuate con lo smartphone Android smarrito attraverso questa pagina: myaccount.google.com/device-activity.

[2] *Android, alcuni smartphone hanno un malware preinstallato a livello firmware: ecco quali*, *TecnoAndroid*

Successivamente, **recarsi immediatamente presso le Autorità per sporgere regolare denuncia, allegando alla stessa il codice IMEI dello smartphone/tablet** (generalmente è scritto sulla scatola). Il codice IMEI identifica univocamente il dispositivo ed è necessario per richiedere il blocco dello stesso all'operatore di telefonia (maggiori informazioni qui: www.fastweb.it/smartphone-e-gadget/cos-e-e-come-trovare-il-codice-imei/).

Nella denuncia è bene allegare anche il numero telefonico dell'eventuale SIM inclusa ed eventuali servizi presenti sullo smartphone (es. *Home banking)*.

A questo punto possiamo recarci, denuncia alla mano, a **una filiale del nostro operatore di telefonia mobile (TIM, Vodafone, 3...) e richiedere un "cambio carta SIM"**: questa procedura, che ha generalmente un costo di qualche euro, vi permetterà di ottenere **una nuova SIM attestata sul medesimo numero**, così da evitare che possa essere usato indebitamente.

In caso di furto o smarrimento di SIM e/o terminale istituzionale...

Nel caso del **furto o smarrimento di un terminale e/o una SIM istituzionale**, contattare immediatamente il servizio di assistenza via e-mail a helpdesk@unisi.it, allegando copia della denuncia effettuata presso le Autorità e contenente, nel caso, il codice IMEI del terminale sottratto (i dati sono recuperabili dal portale voip.unisi.it, previa autenticazione via *unisiPass*).

Nell'eventualità che il terminale contenesse materiale contenente dati personali o particolari, informazioni riservate o documenti istituzionali dell'Università di Siena non destinati alla divulgazione, è necessario darne subito comunicazione via mail all'indirizzo abuse@unisi.it così da attivare le procedure in caso di *data breach*.

CSIRT - Computer Security Incident Response Team - Ufficio esercizio e tecnologie

Università di Siena – Via S. Bandini 25, SIENA

helpdesk@unisi.it // +39 0577235000

Riferimenti

La normativa europea sulla protezione dei dati personali ("GDPR") impone la definizione di contromisure atte a minimizzare la possibilità del furto di dati ("*data breach*") e le eventuali conseguenze.

La rete Internet è diventata strumento indispensabile per l'espletamento di gran parte delle attività lavorative dell'Ateneo. Attraverso la Rete, l'Ateneo permette agli studenti, ai docenti, ai ricercatori, ai tecnici, agli amministrativi, ai collaboratori e a tutto il restante personale, l'accesso ai dati e ai servizi necessari allo svolgimento delle attività didattiche e amministrative. La sicurezza dei dati e delle infrastrutture assume, pertanto, un ruolo essenziale per le libertà e i diritti degli interessati e per il mantenimento della *business continuity*.

Qualsiasi dispositivo connesso in Rete diventa attore del processo di business e deve rispettare alcuni requisiti minimi per la salvaguardia dell'infrastruttura ICT e dei suoi servizi.

- ➔ **Garante per la protezione dei dati personali** - Regolamento europeo in materia di protezione dei dati personali - www.garanteprivacy.it/regolamentoue
- ➔ **Agenzia per l'Italia digitale** - Misure minime di sicurezza ICT per le PA - www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict
- ➔ **Garante per la protezione dei dati personali** interviene sull'utilizzo dello smartphone e tutela dei dati - www.garanteprivacy.it/temi/smartphone

Contatti e siti web utili

- ➔ Gestione delle **credenziali unisiPass** e **aggiornamento password**: my.unisi.it
- ➔ **Avvisi di sicurezza** dell'Università di Siena: www.uet.unisi.it/category/sicurezza/
- ➔ Servizio di **assistenza tecnico-informatica** dell'Università degli Studi di Siena: helpdesk@unisi.it