# QUALCHE CONSIGLIO PER ESSERE IN INTERNET IN SICUREZZA

### Una soluzione di sicurezza affidabile

- Preferisci delle suite di sicurezza complete ai semplici antivirus (soprattutto se sono gratuiti): le suite offrono più funzioni per la tua sicurezza.

### Fa regolarmente il backup dei dati

- Crea dei backup in un cloud protetto o su un hard disk esterno e scollegalo quando il backup è stato completato.

### Aggiorna i tuoi dispositivi

- Attiva le opzioni di aggiornamento automatico nelle impostazioni di Windows, macOS, Android e iOS.

### Installa le applicazioni solo tramite i siti o gli store ufficiali

- Su dispositivo mobile, usa l'App Store o Google Play. Per Windows, vai nei siti Internet delle aziende di informatica.

### Usa una password diversa per ogni servizio

- Una funzione Password Manager gestisce automaticamente nomi utente diversi e protetti.

### Attiva la doppia autenticazione quando è possibile

- La doppia autenticazione può avvenire tramite SMS o app su dispositivo mobile.

### Evita le reti Wi-Fi pubbliche o sconosciute

- Usa una VPN per crittografare il traffico e proteggere i tuoi dati.

### Non fidarti di chiavette e dischi USB

- Alcuni antivirus analizzano il contenuto dei dischi USB per una maggiore sicurezza.

# PERCHÉ PROTEGGERSI CONTRO LE MINACCE ONLINE?

## 18750 nuovi virus

e minacce compaiono su Internet ogni ora

## Un riscatto di € 650,00

è la somma da pagare in media per recuperare i dati presi in ostaggio dagli hacker

## 2,1 milioni di nuovi siti

di phishing individuati ogni mese



(1) Bitdefender Internet Security, janeiro de 2024 https://www.av-comparatives.org/tests/summary-report-2023/
(2) https://www.av-test.org/en/antivirus/home-users/
(3) https://www.pcmag.com/reviews/bitdefender-total-security

Bitdefender / FERRARI TEAM PARTNER

# Bitdefender

## I RISCHI SU INTERNET

## SPIEGAZIONI E CONSIGLI

## IN CHE MODO PROTEGGERSI?

**Trusted. Always.**

# FALSI SUPPORTI TECNICI

Il fine delle truffe messe in atto dai servizi fasulli di assistenza tecnica è spaventare le persone. Il cybercriminale ti contatta via SMS, telefono, chat, e-mail, o attraverso un messaggio pop-up sul tuo computer. Ti informa di un grave problema tecnico e di un rischio di perdita di dati per convincerti a chiamare un numero di telefono per avere assistenza*. Dopo aver preso il controllo della macchina e aver fatto finta di risolvere il problema e installare software o sottoscrivere abbonamenti, il cybercriminale cercherà anche di sottrarti del denaro chiedendoti le tue coordinate bancarie.

## TRUFFE TRAMITE FALSA ASSISTENZA TECNICA

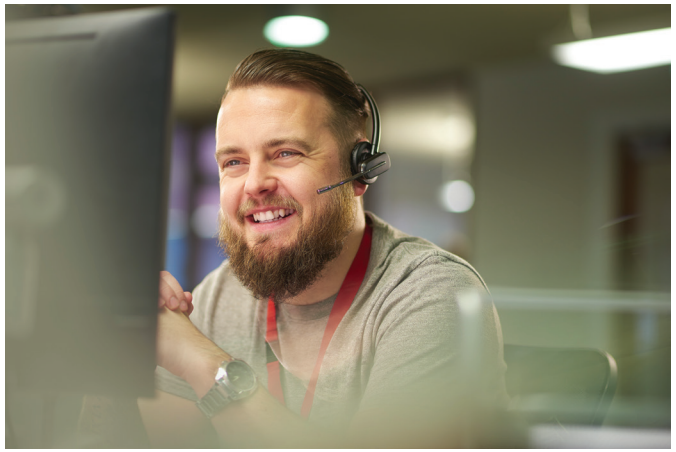
Il tuo computer è bloccato e ti viene chiesto di chiamare un servizio di assistenza tecnica? Sei vittima di una truffa da parte di un servizio fasullo di assistenza tecnica!

### SCOPO

Indurre la vittima a pagare uno pseudo-intervento informatico e/o a farle sottoscrivere abbonamenti a pagamento.

### TECNICA

Far credere che ci sia un problema tecnico grave che implica il rischio di perdere i dati o di non poter usare il dispositivo (tramite monitor bloccato, telefonata, SMS, e-mail, ecc.).



### CONSIGLI

- Non rispondere mai a messaggi e chiamate di gente che non conosci
- Conserva tutte le prove
- Riavvia il dispositivo
- Fai un'analisi antivirus
- Modifica tutte le password
- Se hai pagato, contatta la tua banca e revoca l'autorizzazione al pagamento
- Sporgi denuncia

# I RANSOMWARE

Il ransomware è un software maligno che blocca l'accesso al tuo dispositivo o ai tuoi file criptandoli. Il cybercriminale richiede il pagamento di un riscatto per potervi accedere nuovamente. Il dispositivo può essere infettato da un ransomware dopo aver aperto un allegato, o aver cliccato su un link maligno ricevuto nelle e-mail, o a volte semplicemente navigando su siti web compromessi, o anche dopo un'intrusione nel tuo sistema.

## RANSOMWARE

Non puoi più accedere ai tuoi file e ti viene chiesto un riscatto?
Sei vittima di un attacco tramite ransomware!

### SCOPO

Esigere il pagamento di un riscatto per rendere l'accesso ai file bloccati.

### TECNICA

Blocco dell'accesso ad alcuni dati tramite l'invio di un messaggio che contiene link o allegati maligni o mediante intrusione nel sistema.


### CONSIGLI

- Scollega la macchina da Internet e dalla rete locale
- Non pagare il riscatto
- Sporgi denuncia
- Fatti assistere da professionisti o da consulenti esperti
- Ripristina i dati partendo dai backup creati

# IL PHISHING

Il phishing è una frode progettata in modo che il cybercriminale finge di essere una persona di cui ti fidi al fine di ingannarti e indurti a fornire i tuoi dati personali, come nomi utente, password e/o coordinate bancarie. Può trattarsi di un falso messaggio, un SMS o una telefonata da una banca, un social network, un operatore telefonico, un fornitore di energia, un sito di shopping online, un'amministrazione pubblica, ecc.

## TENTATIVI DI PHISHING

Ricevi un messaggio o una chiamata inattesa, se non allarmante, da una organizzazione nota e all'apparenza ufficiale che ti chiede delle informazioni personali o bancarie? Forse sei vittima di un attacco tramite phishing!

### SCOPO

Rubare informazioni personali o professionali (identità, indirizzi, account, password, dati bancari, ecc.) per farne un uso fraudolento.

### TECNICA

Truffa inviata tramite un falso messaggio, SMS, a volte per posta o tramite telefonata da amministrazioni, banche, operatori, social network, siti di e-commerce...

### CONSIGLI

- Non comunicare mai informazioni sensibili in seguito a un messaggio o a una telefonata
- Al minimo dubbio, contatta direttamente l'ente interessato per avere conferma
- Revoca immediatamente l'autorizzazione al pagamento (in caso di truffa bancaria)
- Modifica le password divulgate
- Sporgi denuncia
- Segnala il fatto nei siti specializzati (vedere link utili)