



**LA LEGGE PER TUTTI**  
INFORMAZIONE E CONSULENZA LEGALE

# **È possibile essere spiati dalla webcam o fotocamera?**

Autore: Mariano Acquaviva | 26/08/2021



*Virus e malware che si introducono nei dispositivi prendendo il controllo della telecamera: come difendersi? Quali reati si commettono?*

La tecnologia ci aiuta nella vita di tutti i giorni, rendendo possibile cose che, solo qualche anno fa, sembravano realizzabili solo in un film di fantascienza. La grande importanza delle moderne innovazioni si è fatta apprezzare ancor di più durante l'emergenza pandemica quando, non potendo uscire di casa, siamo stati costretti a

vedere amici, seguire seminari, ordinare beni e lavorare tramite Internet. Ogni cosa, però, ha un prezzo da pagare e, probabilmente, quello che tutti devono alla tecnologia è la parziale rinuncia alla propria riservatezza. Anche quando non lo vogliamo, la nostra privacy potrebbe essere sotto attacco da parte di malintenzionati che si avvalgono di competenze e prodotti specifici per violare i sistemi di sicurezza e intrufolarsi nelle nostre vite. Con questo articolo vedremo se **è possibile essere spiati dalla webcam o dalla fotocamera** dello smartphone.

L'argomento è salito prepotentemente agli onori della cronaca per via delle numerose **truffe** che molti italiani hanno subito. In pratica, si tratta di messaggi (generalmente recapitati via email) con cui il destinatario viene ricattato: se non paga una determinata somma, il video che la webcam o la fotocamera hanno ripreso a insaputa della vittima verrà messo in Rete, in modo che tutti possano vederlo. Il più delle volte, si tratta di un'estorsione che si basa sul nulla: il malintenzionato non ha alcun video, ma gli conviene far credere il contrario per poter ricattare il malcapitato.

Il problema è che una cosa del genere, cioè prendere il controllo delle periferiche di pc e smartphone, è possibile. Esistono davvero strumenti che consentono di poter azionare a propria insaputa l'occhio del cellulare o del computer per riprendere di nascosto ciò che accade intorno. **È possibile essere spiati dalla webcam o fotocamera?** Come tutelarsi? Scopriamolo insieme.

## **Webcam: come si spia una persona?**

Introdursi abusivamente nella webcam di un computer non è cosa impossibile per gli **hacker**: è sufficiente un **virus** e il gioco è fatto.

In casi del genere, si parla di **camfecting** (combinazione delle parole "camera" e "infetto"), termine che indica il processo di hackeraggio della webcam di una persona che consente di attivarla senza il permesso del proprietario e a sua insaputa.

La webcam azionata a distanza può essere utilizzata per guardare qualsiasi cosa all'interno del campo visivo della telecamera, con ovvia violazione della **privacy** del proprietario.

La tecnologia di **malware** e virus che consente a un hacker di visualizzare direttamente attraverso la webcam è chiamata **Rat**, acronimo che sta per “Trojan di accesso remoto”.

I malware sui dispositivi infetti possono registrare qualsiasi cosa, dai tasti ai file salvati sul disco rigido e **registrare video dalla webcam**.

Ovviamente, per prendere il controllo del computer e della camera occorre che il proprietario del pc presti, anche inconsapevolmente, il consenso a introdurre il virus nel proprio pc. Ciò può accadere cliccando su un **link ingannevole**, aprendo o rispondendo a un’email, effettuando il **download** di un file sospetto.

Insomma: l’hacker non può spiare una persona tramite webcam se la vittima non ha in qualche modo “aperto” l’ingresso del software malevolo.

## **Fotocamera smartphone: come spiare una persona?**

Quanto detto per la webcam del pc vale anche per la fotocamera dello **smartphone**: tramite virus il malintenzionato si intrufola nel dispositivo e riesce a prenderne il controllo, accedendo a tutte le funzionalità del cellulare, inclusa la fotocamera.

Finora, abbiamo visto come accedere al dispositivo altrui da remoto, cioè mediante trasmissione di un software malevolo che entra nel pc o nello smartphone all’insaputa del proprietario. Lo stesso risultato può però essere ottenuto mediante la modifica “fisica” dell’apparecchio. Ciò accade soprattutto con i cellulari, più piccoli e facili da manomettere.

Una persona particolarmente esperta (un tecnico, ad esempio) che ha accesso materiale al dispositivo potrebbe installare manualmente uno **spyware** (software malevolo) in grado di leggere i messaggi, scattare foto ed effettuare riprese con la fotocamera del cellulare.

La maggior parte delle volte, però, il controllo della fotocamera è assunto da remoto, approfittando del fatto che il titolare, involontariamente, ha scaricato un programma che all’interno conteneva un malware.

# Spia tramite webcam e fotocamera: come difendersi?

Prevenire è meglio che curare. Per **difendersi da software spia** che sono in grado di controllare la webcam del pc o la fotocamera dello smartphone è opportuno adoperare tutti gli strumenti tipici di chi intende difendersi dai malware:

- effettuare solo **download sicuri**, evitando quindi siti sospetti e applicazioni gratuite di dubbia provenienza;
- dotarsi di un buon **antivirus**;
- sottoporre periodicamente il dispositivo a controllo da parte di un tecnico esperto.

In ogni caso, un metodo piuttosto sicuro per impedire all'occhio della camera di effettuare riprese indesiderate è quello di coprirlo, magari con del **nastro adesivo**. Ciò può essere fatto senza problemi con la webcam del pc. In questo modo, si avrà almeno la certezza che, seppur manomessa, la telecamera non riprenderà senza il consenso del proprietario.

# Spiare con webcam e fotocamera: quali reati?

Quasi inutile ricordare che **spiare una persona** mediante webcam o fotocamera del cellulare costituisce un illecito, sia civile che penale. Sotto quest'ultimo punto di vista, l'hacker che prende il possesso del dispositivo altrui rischia di commettere almeno uno dei seguenti delitti:

- **interferenze illecite** nella vita privata **[1]**, in quanto il pirata informatico, accedendo alla telecamera e captando suoni e video, effettua una vera e propria intercettazione illegale;
- **accesso abusivo** a un sistema informatico o telematico, in quanto l'hacker è in grado di accedere al dispositivo di altri senza averne il consenso **[2]**;
- detenzione e **diffusione abusiva** di codici di accesso a sistemi informatici o telematici, se il malintenzionato diffonde in rete le password e credenziali della vittima **[3]**;

- **violazione di corrispondenza**, se l'hacker, attraverso il malware, accede alle email e ai messaggi riservati **[4]**;
- **estorsione [5]**, quando il pirata ricatta la vittima chiedendogli denaro in cambio del segreto sulle riprese effettuate abusivamente.

Di conseguenza, chi sia vittima di una di queste condotte potrà recarsi presso qualsiasi presidio delle forze armate e sporgere **denuncia/querela**. Generalmente, di tali crimini si occupa la **polizia postale**.

## **Note**

**[1]** Art. 615-bis cod. pen. **[2]** Art. 615-ter cod. pen. **[3]** Art. 615-quater cod. pen.  
**[4]** Art. 616 cod. pen. **[5]** Art. 629 cod. pen.