Een webcam in huis, waar moet je op letten?

Bijna alle toestellen hebben tegenwoordig een ingebouwde camera. Dit is zeer handig, maar brengt ook enkele risico's met zich mee.

Wanneer je toestel besmet is met een virus kunnen criminelen de controle over je toestel overnemen en je webcam zonder jouw medeweten inschakelen (het lichtje van je camera kan ook uitgeschakeld worden). Ze kunnen zo foto's nemen zonder je medeweten. Als je toestel bijvoorbeeld in je slaapkamer staat, kunnen foto's genomen worden wanneer je je omkleedt, en gebruiken om je af te persen.

Toestellen

Dit is het geval voor je computer, smartphone, tablet, maar ook je smart-tv, babyfoon en andere toestellen met een camera in en die verbonden zijn met internet.

Gezond verstand en enkele simpele tips kunnen dit voorkomen.

TIPS:

- uit voorzorg kan je je webcam afplakken met een post-it of een herbruikbare webcamcover als je camera niet actief is. We geven voor safer internet day hieronder gratis herbruikbare webcamcovers weg, zolang de voorraad strekt.
- Gebruik een virusscanner en scan regelmatig je toestel op virussen.
- Vaak hebben toestellen zoals babyfoons, smart-tv's, printers, Wifi-routers, ook een standaard wachtwoord. Verander de standaard wachtwoorden op je toestellen in een moeilijk te raden wachtwoord. (meer tips vind je op de pagina over het maken van veilige wachtwoorden) Voor de meeste toestellen vind je uitleg op de website van de fabrikant hoe je het wachtwoord moet veranderen.
- Wees voorzichtig met bepaalde websites of applicaties die toegang vragen tot je webcam.
- Download enkel officiële programma's of applicaties op je toestel.
- Meestal kan je in de instellingen van je toestel nakijken aan welke websites of applicaties je toestemming hebt gegeven
- Zorg dat je steeds de laatste versie je camera programma (bv. Skype, Facetime, je webcamprogramma…) gebruikt, en zo niet, update je programma.