Diputació de València | Protecció de Dades i Seguretat de la Informació

Butlletí DivalData

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 37| Juliol 2023

RECOMANACIONS DE SEGURETAT PER Al PERÍODE VACACIONAL

ÍNDEX

RECOMANACIONS DE SEGURETAT PER AL PERÍODE VACACIONAL

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpto. de Protecció de Dades i Seguretat de la Informació

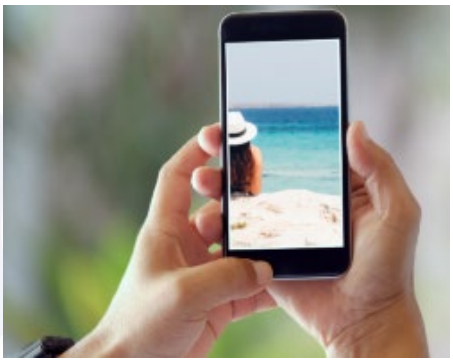
Pl. de Manises, 4 46003 València

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç

INTRODUCCIÓ



Amb l'arribada de l'estiu, comença l'època de vacances per a molts de nosaltres. Malgrat ser dies de desconnexió del treball i de connexió amb la nostra família, amics i les nostres aficions, hem de continuar implementant rutines segures en l'ús dels nostres dispositius. I és que, en aquesta època, es produeix un augment significatiu dels ciberatacs, que podrien posar en perill les nostres dades personals o, fins i tot, aquells dels quals la nostra organització és responsable. És per això que, no podem baixar la guàrdia i hem de continuar sent actius en la protecció de dades, afrontant les situacions de risc que es presenten.

En el present butlletí us presentem alguns consells sobre com afrontar aquestes situacions per a la protecció de les dades personals en època estival.

RECOMANACIONS DE SEGURETAT PER Al PERÍODE VACACIONAL

1. XARXES WIFI PÚBLIQUES

Les xarxes Wifi públiques són aquelles que no estan protegides per una contrasenya i ens permeten connectar-nos a internet d'una forma còmoda i ràpida. També són aquelles a les quals, fins i tot tenint contrasenya d'accés, es connecten molts usuaris. Aquestes no xifren la informació que es transmet a través d'elles, per la qual cosa no són segures. Malgrat els seus avantatges, un dels seus principals inconvenients és la seua naturalesa oberta i accessible, la qual cosa pot comprometre la informació de la nostra organització.

En cas d'accedir de manera puntual als serveis o aplicacions de la Diputació de València quan estem de vacances -el que ens portaria a connectar-nos a aquesta mena de xarxes en hotels, aeroports, cafeteries, etc.- segueix aquestes recomanacions de seguretat:

- **No et connectes a xarxes sense fils obertes.** Tant l'administrador com algun dels usuaris connectats poden utilitzar tècniques per a robar-nos informació.
- **És preferible que et connectes a la xarxa 3G/4G/5G de l'operador de telefonia**. Hui dia qualsevol operador ofereix una quantitat notable de GB per a trànsit de dades.
- En cas de necessitat, **si et connectaràs a una xarxa sense fil pública, és preferible accedir a una xarxa amb seguretat WPA o WPA2.** Les xarxes obertes i amb seguretat WEP són totalment insegures. Consulta els detalls de la xarxa Wifi per a comprovar davant quin tipus de xarxa estàs.
- **Comprova** que la xarxa gratuïta disponible és **l'oficial** del lloc en el qual estàs.
- Sempre que estiguen disponibles, connecta't a pàgines amb **certificat de seguretat https://**
- **No inicies sessió en cap servei** mentre estigues connectat a una xarxa pública.
- **Evita realitzar transaccions bancàries, compres en línia** o qualsevol altra tasca que supose l'intercanvi de dades des de xarxes Wifi públiques.
- **Deshabilita qualsevol procés de sincronització** del teu equip si usaràs una xarxa pública.
- Mantingues sempre **l'equip actualitzat i l'antivirus instal·lat** correctament.
- Després de la connexió, **elimina les dades de la xarxa memoritzats** pel teu equip.

2. CONTRASENYES

Un dels mecanismes d'autenticació més utilitzats per a protegir l'accés als dispositius, aplicacions i, en general, a la informació, són les contrasenyes. Aquestes són una forma d'autenticació que utilitza informació secreta per a controlar l'accés a algun recurs, constituint la primera línia de contenció per a evitar ciberatacs. Per això, per a no posar en risc la informació continguda en els nostres sistemes o els sistemes d'informació de la nostra organització, durant les nostres vacances hem d'assegurar-nos d'haver creat claus segures i fer un bon ús d'aquestes.

A continuació, oferim una sèrie de recomanacions de seguretat:

- **No** utilitzes les contrasenyes que se't proporcionen **per defecte.**
- Les contrasenyes han de ser **robustes** (més de 8 caràcters i que continga lletres, números i símbols).
- **No** han de ser **les mateixes les empleades en l'àmbit personal i** les empleades per a l'accés els sistemes o aplicacions **en l'àmbit laboral.**
- **No compartisques les teues contrasenyes.**
- **No** mantingues les teues contrasenyes per escrit a la vista o a l'abast de tercers.
- **No** utilitzes les **credencials d'accés d'altres** usuaris, encara que disposes de l'autorització del seu titular.
- **Evita** utilitzar el **recordatori de contrasenyes.**
- Si reps una **trucada telefònica o missatge sol·licitant el teu usuari i contrasenya, mai els facilites.**
- Utilitza un **gestor de contrasenyes segur.**

3. ATACS D'ENGINYERIA SOCIAL. *PHISHING*.

En època estival augmenten els ciberatacs, especialment, de phishing. Aquesta és una de les tècniques d'enginyeria social més utilitzades pels ciberdelinqüents per a obtindre informació personal dels usuaris suplantant a una persona o entitat.

La tècnica consisteix en l'enviament d'un missatge o la realització d'una crida, per part d'un ciberdelinqüent, a un usuari simulant ser una persona o una entitat de confiança amb l'objectiu enganyar-li i manipular-li, a fi que acabe realitzant alguna acció, que pot en perill les seues dades personals o els de l'organització a la qual pertany.

Hem de tindre especial cautela, ja que, com indicàvem, aquesta és una època en la qual rebem molts emails d'empreses per a confirmar la reserva d'una habitació d'hotel, el pagament d'un cotxe de lloguer o la compra d'un bitllet d'avió, que podrien portar a confusió, per la qual cosa hem de prestar especial atenció. En qualsevol cas, no haguérem d'utilitzar el correu electrònic corporatiu per a aquesta mena de menesters.

A continuació, oferim una sèrie de recomanacions de seguretat per a protegir-nos enfront del phishing:

- Si el missatge et demana fer alguna **acció estranya, ignora'l.**
- Si el missatge t'obliga a prendre una **decisió en poc temps, és mal senyal.**
- **Comprova el domini del correu remitent** i que el seu nom coincidisca amb el seu compte de correu.
- **Evita obrir arxius adjunts si desconeixes el remitent o no esperes el document.**
- **Sospita** de missatges amb **faltes d'ortografia, errors gramaticals i salutacions genèriques.**
- Ves amb **compte** amb les **sol·licituds de dades a través de webs a les quals has arribat seguint l'enllaç**. Millor accedeix directament a la web de l'organització.
- Mantingues **actualitzat el navegador, el sistema operatiu i altre programari.**
- **Evita** l'ús de **mitjans extraïbles.**

4. CODIS QR

Les inicials de QR es tradueixen de l'anglés *Quick Response*, literalment, com a 'resposta ràpida'. Aquests serveixen per a emmagatzemar informació i fer-la més accessible als usuaris. Hui dia, a través de qualsevol cambra d'un telèfon intel·ligent o tauleta es poden escanejar aquests codis per a accedir directament, per exemple, a una pàgina web o descarregar una aplicació. Molts llocs d'interés o hostaleria utilitzen aquest tipus de codis perquè les persones puguen accedir ràpidament a la informació del lloc com, per exemple, la carta d'un restaurant.

No obstant això, cal tindre precaució a l'hora d'escanejar aquests codis, ja que podrien portar-nos a enllaços o a la descàrrega d'aplicacions no desitjades, capaces d'explotar fallades de seguretat del sistema operatiu i obtindre la informació emmagatzemada en el dispositiu.

El seu ús ha de realitzar-se de manera segura, per exemple, amb una eina gratuïta per a analitzar la URL, verificant que és la correcta i no està manipulada.

A continuació, et proporcionem algunes recomanacions que pots aplicar:

- Si a primera vista la **URL** ens sembla **sospitosa**, directament **no hem d'accedir a ella.**
- Assegurar-nos que la web a la qual accedirem sempre compleix amb **estàndards de protecció i navegació segura**, com, per exemple, que tinga **HTTPS.**
- Fer ús d'**analitzadors d'enllaços**. L'Institut Nacional de Ciberseguretat recomana alguns com VirusTotal i URLVoid. D'aquesta manera, abans d'obrir la web podrem comprovar que no es tracta de cap atac d'enginyeria social.
- També podem recórrer a **aplicacions,** com Kaspersky QR Scanner, disponible en Android i iOS, que realitzen una sèrie de revisions mèdiques de seguretat abans d'activar el codi QR en el telèfon intel·ligent.
- **No proporcionar cap dada privada ni cap contrasenya, personal o professional,** a pàgines web que hàgem accedit a través d'un codi QR. És convenient que si accedim a pàgines de bancs o botigues en línia on introduïm dades de la nostra targeta bancària, ho fem des de la URL completa o a través de la seua aplicació pròpia.

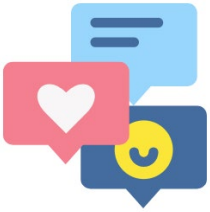
5. PROTECCIÓ DE DISPOSITIUS

Quan viatgem o realitzem activitats estiuenques com anar a la piscina, la platja o visitar llocs turístics, augmenten els riscos de perdre o que ens sostraguen els nostres dispositius portàtils (ordenadors, mòbils, tauletes). Aquests dispositius contenen multitud d'informació personal, nostra o, en molts casos, informació que podria comprometre a la nostra organització -per exemple, en cas que en alguna ocasió s'haja utilitzat el dispositiu personal per a consultar informació professional o fer alguna tasca professional i s'haja mantingut la mateixa en el dispositiu, o en cas d'haver introduït en el mateix les credencials de la nostra organització i no s'hagen eliminat després-.

A continuació, oferim una sèrie de recomanacions de seguretat per a protegir els teus dispositius:

- Utilitza un **sistema de clau o patró** per a **bloquejar els dispositius**.
- **Evita compartir els dispositius** amb familiars, amics i estranys.
- **Bloqueja'ls** quan no estiguen en ús.
- Guarda els **documents sensibles i confidencials** en un **lloc segur.**
- **No** connectes dispositius **USB desconeguts.**
- **No** deixes **dispositius mòbils desatesos o visibles en llocs públics.**
- **No** utilitzes **carregadors públics.**
- **Actualitza el *software*** al més prompte possible.

6. SHARENTING



En època de vacances s'augmenta l'ús de les xarxes socials per a compartir moments entre les famílies i amics. Moltes persones han trobat en aquestes plataformes el lloc idoni per a publicar fotos i vídeos de diferents moments de la vida dels menors, acompanyats de comentaris (entre els quals es pot trobar el nom o l'edat), contribuint a alimentar la seua empremta digital, sense comptar que els seus fills pot ser que no estiguen d'acord el dia de demà..

El *sharenting* va créixer de manera exponencial durant el confinament i la seua pràctica és habitual en aquesta època, per la qual cosa és important reflexionar abans de publicar aquest tipus de continguts en la xarxa. Per a això, és convé recordar algunes recomanacions per al seu ús:

- Tenim l'obligació de cuidar la seua imatge i intimitat. Les persones menors d'edat tenen drets que han de ser protegits de manera especial.

- És possible que no siguem conscient de com s'estan difonent les imatges. No sempre és fàcil entendre i gestionar la lògica i els canvis de gestió de privacitat de les xarxes socials.

- Existeixen altres formes més segures per a compartir imatges. És necessari limitar amb qui compartir la informació i triar la plataforma adequada.

- Habitualment, es comparteix més informació que la que s'aprecia a simple vista. Una imatge innocent pot contindre detalls de context importants i fins i tot geolocalització.

- En compartir les imatges amb altres persones, aquestes poden assumir que això significa que les poden publicar i que les imatges no són tan privades. Sense mala intenció, de manera directa o indirecta, poden expandir l'abast i fins i tot fer-les públiques.

- Compartir imatges d'altres persones sense el seu consentiment pot ser una infracció de la normativa de protecció de dades. No és un bon exemple per a ningú, menys encara per als menors d'edat.

7. TECNOLOGIES EN MENORS

Si tens fills adolescents, l'estiu pot ser l'època on més temps passen amb els seus dispositius, ordinadors, tauletes i mòbils. A més, durant gran part d'aqueix temps fan ús de les seues xarxes socials compartint fotos i continguts que no sempre són els més adequats.

Per això, és recomanable tindre una sèrie de mesures o pautes a l'hora de permetre l'ús d'aquests dispositius en la llar:

- El **control parental** és un mecanisme per a controlar en diferents llocs web, sistemes operatius o equips l'accés i ús que els menors d'edat li donen a internet. A través del control parental podem monitorar la navegació, restringir continguts no aptes per a menors i bloquejar pàgines o usuaris que puguen ser una amenaça per als xiquets.

- A més, és possible establir **límits de temps** en el qual els menors poden estar amb l'ordinador encés, evitar que juguen o accedisquen a unes certes aplicacions i jocs o impedir que executen uns certs programes.

- També, en **xarxes socials** com Facebook, Twitter o Instagram **si alguna publicació no és apta** perquè un menor d'edat la veja, es pot **reportar** i el contingut desapareixerà de la línia de temps.

Fer d'internet un espai segur per als nostres xiquets és a les nostres mans. No els descurem mentre naveguen en la xarxa.

"A l'estiu es produeix un augment significatiu de les ciberamenazas, que podrien posar en perill les nostres dades personals o, fins i tot, aquells dels quals la nostra organització és responsable. Per a protegir-los, segueix aquests consells de seguretat: no et connectes a xarxes sense fils obertes; abans d'anar-te de vacances, assegura't d'haver creat claus segures i fes un bon ús d'aquestes; para atenció als correus electrònics, missatges o crides rebudes, analitzant el seu contingut abans de proporcionar informació; tingues precaució a l'hora d'escanejar codis QR, ja que podrien portar-nos a enllaços o a la descàrrega d'aplicacions no desitjades, capaces d'obtindre la nostra informació; protegeix els teus dispositius amb clau i no els deixos desatesos en llocs públics; vigila que els teus fills no facen un ús inadequat dels dispositius".

MATERIAL COMPLEMENTARI

- Protecció de dades en vacances (AEPD). Pots consultar la infografia en aquest enllaç.
- Protecció de dades en vacances (AEPD). Pots consultar l'article en aquest enllaç.
- Consells de ciberseguretat durant les vacances (APDCAT). Pots consultar l'article en aquest enllaç.
- Consells per a unes vacances cibersegures (INCIBE). Pots consultar l'article en aquest enllaç.
- Prepara't per a gaudir d'unes vacances cibersegures en família (INCIBE). Pots consultar l'article en aquest enllaç.
- Escaneja codis QR de manera fiable i segura (INCIBE). Pots consultar l'article en aquest enllaç.
- Deu recomanacions de ciberseguretat per a les vacances (GVA). Pots consultes l'article en aquest enllaç.

NOTÍCIES

- **La AEPD publica una Circular sobre el dret dels usuaris a no rebre anomenades comercials no sol·licitades.** La circular fixa els criteris conforme als quals actuarà l'Agència en aplicació de l'article 66.1.b) de la Llei General de Telecomunicacions, que implica canvis per a poder realitzar aquest tipus de crides i que s'aplica des del 29 de juny. Pots consultar la Circular en aquest enllaç.

- **La L'AEPD sanciona a l'organitzadora del Mobile World Congress en 2021 per utilitzar dades biomètriques dels assistents sense haver realitzat adequadament una Avaluació d'Impacte en Protecció de Dades.** L'AEPD considera que la recollida de dades biomètriques en el reconeixement facial establit per a la identificació dels assistents al Congrés degué comptar amb una Avaluació d'Impacte de Protecció de Dades. Pots consultar la Resolució en aquest enllaç.

- **El TJUE obri la porta a revelar la identitat dels empleats que consulten dades personals.** El Tribunal de Justícia de la Unió Europea (TJUE) determina que qualsevol persona té dret a saber la data i les raons per les quals una entitat ha consultat les seues dades personals, i obri la porta a revelar la identitat dels treballadors que ho van fer quan siga indispensable per a permetre a l'interessat exercir efectivament els drets que li confereix la normativa i sempre sota la condició que es tinguen en compte els drets i llibertats dels empleats. Pots consultar la Sentència en aquest enllaç