pimec

Micro, petita i mitjana
empresa de Catalunya

Consells de
CIBERSEGURETAT PER A PIMES

pimec.org

FER CÒPIA DE SEGURETAT

... això evitarà qualsevol pèrdua de dades per robatori, incendi, altres danys físics o ransomware.

- Identifiqui el que **necessita guardar**. Les còpies de seguretat han de formar part del dia a dia de l'empresa.
- Comprovi que es poden **restaurar** les còpies de seguretat.
- Asseguri's que el dispositiu que conté la seva còpia de seguretat **no estigui connectat permanentment** al dispositiu que conté la còpia original, ni físicament ni a través d'una xarxa local.

FORMAR I CONSCIENCIAR CONTRA L'ENGINYERIA SOCIAL

... mitjançant la qual s'evitaran la majoria d'atacs en què intervingui el factor humà.

- Informi's sobre els **atacs d'enginyeria social més habituals,** independentment del canal utilitzat (phishing, vishing, SMiShing etc.), on els estafadors demanen informació confidencial.
- Comprovi si hi ha **signes d'engany evidents en el missatge**, com ortografia, pronunciació, gramàtica deficients, o versions de logotips de baixa qualitat.
- Informi els membres de l'empresa que la **informació personal** que comparteixen a Internet pot ser utilitzada per realitzar atacs dirigits d'enginyeria social.
- Tingui desactivada per defecte l'opció "**compres per Internet**" de totes les targetes de crèdit de l'empresa, i activi-la només en el moment de realitzar un pagament.
- **No castigui** el personal si ha sigut víctima d'un atac, ja que altres evitaran informar-ne en un futur.

MANTENIR SEGURS ELS TELÈFONS INTEL·LIGENTS (I TAULETES)

... necessiten encara més protecció que els equips d'escriptori, ja que s'usen fora de la seguretat de l'oficina.

- Utilitzi una solució **antivirus** per protegir també els seus dispositius mòbils.
- Activi la **protecció d'accés per a dispositius mòbils**, amb contrasenya, PIN o reconeixement d'empremtes digitals.
- Configuri la **gestió remota** dels dispositius. En cas de pèrdua o robatori, podran ser rastrejats, esborrats o bloquejats remotament.
- Activi l'opció d'**actualització automàtica** per mantenir actualitzats els seus dispositius i aplicacions instal·lades.
- **Substitueixi** els dispositius que ja **no disposen de suport** per part dels venedors i busqui altres alternatives.
- No es connecti a **punts d'accés públic de wifi**, utilitzi connexions 3G, 4G o VPN.

PREVENIR EL DANY PER PROGRAMARI MALICIÓS (MALWARE)

...mitjançant l'adopció d'algunes tècniques simples i de baix cost.

- Utilitzi programari **antivirus** en tots els dispositius.
- Instal·li només **programes aprovats i de fonts** conegudes, i eviti que els usuaris descarreguin aplicacions de tercers de fonts desconegudes.
- **Actualitzi tot el programari i el firmware** mitjançant l'actualització automàtica proporcionada pels fabricants i proveïdors.
- Controli l'accés a **mitjans extraïbles**, com targetes SD i memòries USB. Pensi a desactivar ports o a limitar-ne l'accés.
- Tingui especial cura amb els **fitxers adjunts** al correu electrònic, sobretot si són executables (.exe, .com, o .bat).
- Activi el **tallafoc** que inclou el sistema operatiu.

UTILITZAR CONTRASENYES

... ja que és la forma més bàsica d'evitar que persones no autoritzades accedeixin als seus dispositius i dades.

- Asseguri's que tots els dispositius facin servir productes que requereixin una **contrasenya d'inici**.
- Utilitzi l'**autenticació de doble factor** (2FA) sempre que sigui possible.
- Eviti l'ús de **contrasenyes predictibles** (com cognoms i noms de mascotes) i les contrasenyes més comunes que els delinqüents poden endevinar (com password, 12345, etc.).
- Canviï les **contrasenyes predeterminades** dels fabricants abans que es distribueixin al personal.
- Utilitzi un **gestor de contrasenyes** i asseguri's que la contrasenya mestra sigui segura.
- Una **contrasenya segura** ha de tenir números, lletres, símbols (!, $, %, &, #, etc.) i majúscules i minúscules. A més, ha de tenir una longitud mínima de vuit caràcters.

Informació facilitada per Grail Security Systems.

Fonts:

- National Cyber Security Centre (NCSC) - Cyber Security: Small Business Guide
- National Institute of Standards and Technology (NIST) - Small Business Cybersecurity Corner
- European Union Agency for Cybersecurity (ENISA) - Security for Small and medium size enterpris

Més informació:
Imma Navarra | sistemes@pimec.net