Autoavalua la ciberseguretat del teu projecte:

Protecció contra malware i ransomware

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per prevenir i gestionar atacs de malware i ransomware

Recomanacions en ciberseguretat

Abril de 2025

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

Índex de Continguts: protegir-se del malware i el ransomware

Avís de responsabilitat en la prevenció i protecció:
Les recomanacions incloses en aquesta guia tenen com a objectiu proporcionar consells pràctics i senzills per millorar la ciberseguretat del teu negoci. Tot i això, la **responsabilitat** última de la prevenció i protecció dels dispositius, dades i sistemes recau en els usuaris.

Es recomana comptar amb el suport d'un equip tècnic o servei informàtic especialitzat per garantir una implementació adequada de les mesures descrites. A més, assegura't de seguir sempre les instruccions oficials dels fabricants i desenvolupadors de software, aplicacions i dispositius que utilitzis, ja que cada sistema pot tenir requisits específics o actualitzacions que afectin la seva seguretat.

Aquest document no substitueix una auditoria professional de seguretat ni consells específics adaptats a les teves necessitats particulars.

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

1. Introducció

Què són el malware i el ransomware?

Malware (programari maliciós):

El malware és qualsevol programari dissenyat amb la intenció de **danyar**, **infiltrar** o **explotar** dispositius, xarxes o dades. Alguns dels tipus de malware més comuns són:

- **Virus:** Es propaguen infectant fitxers i poden danyar o eliminar dades.
- **Troians:** S'amaguen en programes aparentment legítims i permeten l'accés no autoritzat al dispositiu.
- **Spyware:** Recull informació personal o professional sense consentiment.
- **Adware:** Mostra anuncis intrusius i pot descarregar altres formes de malware.
- **Ransomware:** Una forma específica de malware que xifra els fitxers i exigeix un pagament (rescat) per desbloquejar-los.

Ransomware (programari de segrest):

Aquest tipus de malware xifra els fitxers del dispositiu infectat, fent-los inaccessibles. Els atacants sol·liciten un **pagament en criptomonedes** per restaurar l'accés. El ransomware pot infectar els sistemes a través de:

- Enllaços o fitxers adjunts sospitosos en correus electrònics.
- Descàrregues des de llocs web maliciosos.
- Xarxes o programes sense protecció adequada.

Impacte del malware i ransomware en petites empreses i autònoms

Les petites empreses i els treballadors autònoms són un objectiu atractiu per als atacants perquè sovint no tenen els recursos per implementar mesures avançades de seguretat. Els impactes poden ser devastadors:

1. **Pèrdua de dades essencials:**
   - Arxius de clients, projectes o registres financers poden ser inaccessibles o esborrats.
   - La falta de còpies de seguretat pot agreujar les conseqüències.
2. **Danys econòmics:**
   - El cost mitjà d'un atac de ransomware pot incloure:
     - Pèrdua de productivitat.
     - Despeses en serveis professionals per desinfectar els sistemes.
     - Pèrdua d'ingressos si el negoci no pot operar.
3. **Danys a la reputació:**

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfo si · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- Si les dades de clients es veuen compromeses, pot ser difícil recuperar la confiança.
- Un incident pot generar mala publicitat que afecti el creixement futur.

4. **Compliment normatiu:**
   - Si es perden o es filtren dades personals, poden imposar-se sancions segons regulacions com el RGPD.

Objectius d'aquesta guia

Aquesta guia té com a finalitat ajudar-te a:

- **Comprendre els riscos:** Saber què és el malware i el ransomware i com poden afectar el teu negoci.
- **Prevenir atacs:** Adoptar mesures pràctiques per reduir la probabilitat d'infeccions.
- **Respondre amb eficàcia:** Estar preparat per minimitzar els danys en cas d'incident.

2. Prevenció d'infeccions per malware

Prevenir infeccions per malware és clau per protegir la informació i garantir la continuïtat del negoci. Aquest apartat proporciona mesures pràctiques que petites empreses i autònoms poden implementar fàcilment.

2.1. Instal·lació i ús d'antivirus i antimalware

Els programes antivirus i antimalware són la primera línia de defensa contra el programari maliciós.

- **Característiques essencials d'un bon antivirus:**
  - Escaneig en temps real per detectar amenaces immediatament.
  - Actualitzacions freqüents per protegir-se contra les últimes variants de malware.
  - Opcions per analitzar fitxers i llocs web abans d'obrir-los.
- **Programes recomanats per a petites empreses i autònoms:**
  - Gratuïts: **Avast Free Antivirus**, **AVG Antivirus Free**.
  - De pagament: **Norton 360**, **Bitdefender Total Security**, **Kaspersky Small Office Security**.
- **Consells d'ús:**
  - Configura escaneigs automàtics regulars.
  - Escaneja fitxers i unitats externes abans d'obrir-los.
  - Assegura't que l'antivirus està sempre actiu i actualitzat.

Generalitat de Catalunya · SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

2.2. Com mantenir el sistema operatiu i aplicacions segures

Les actualitzacions periòdiques són essencials per tancar vulnerabilitats que els atacants poden explotar.

- **Actualització del sistema operatiu:**
  - **Windows**: Activa les actualitzacions automàtiques des de **Configuració > Actualització i seguretat**.
  - **macOS**: Configura l'opció "Instal·lar actualitzacions automàtiques" a **Preferències del sistema > Actualitzacions de programari**.
- **Actualització de programes i aplicacions:**
  - Prioritza les aplicacions que gestioni informació sensible (navegadors, programes de correu, eines de gestió).
  - Utilitza botigues oficials per descarregar aplicacions (Google Play Store, Apple App Store).
- **Configuració addicional:**
  - Desactiva aplicacions i serveis que no utilitzis per reduir punts d'accés potencials.
  - Configura un tallafocs per bloquejar connexions no autoritzades

2.3. Bones pràctiques per evitar infeccions per enllaços i descàrregues sospitoses.

Moltes infeccions per malware es produeixen per accions inadvertides de l'usuari, com fer clic en un enllaç o descarregar un fitxer maliciós.

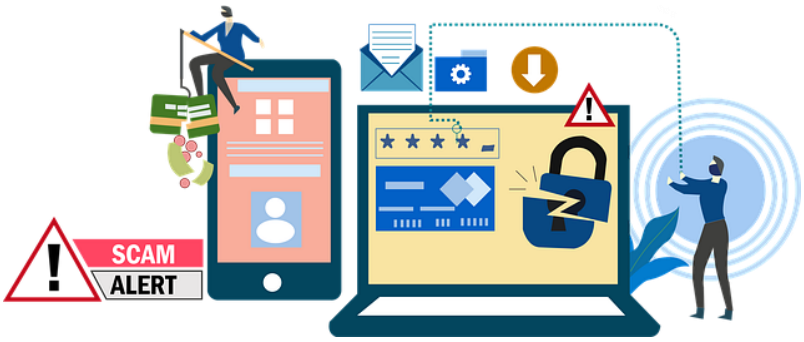
- **Evita enllaços sospitosos:**
  - No facis clic en enllaços d'origen desconegut, especialment en correus electrònics i missatges.
  - Passa el ratolí per sobre de l'enllaç per veure l'adreça completa abans de fer-hi clic.
- **Controla les descàrregues:**
  - Baixa només fitxers de llocs web oficials o de confiança.
  - Comprova les ressenyes i el nombre de descàrregues abans d'instal·lar una aplicació.
- **Escaneja fitxers abans d'obrir-los:**
  - Utilitza l'antivirus per analitzar arxius descarregats.
  - Prova serveis com **VirusTotal** per escanejar fitxers o enllaços en línia.
- **Desconfia de missatges amb urgències falses:**
  - Els atacants sovint creen un sentiment d'urgència per enganyar-te (per exemple, "La teva compte serà bloquejada si no fas clic ara").

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

Beneficis de la prevenció

- **Reducció de riscos:** Implementar aquestes pràctiques disminueix dràsticament les possibilitats d'infecció.
- **Estalvi de temps i diners:** Evites els costos de recuperar dades o reparar sistemes infectats.
- **Confiança i continuïtat:** Protegeixes la teva reputació i mantens el negoci en funcionament.



3. Estratègies per minimitzar l'impacte del ransomware

El ransomware pot tenir conseqüències devastadores, però amb les estratègies adequades pots minimitzar el seu impacte i evitar que els teus fitxers siguin segrestats.

3.1. Què fer per evitar que els fitxers siguin xifrats

- **Bloqueja l'entrada del ransomware:**
  - **No obris correus sospitosos:** El ransomware sovint arriba a través d'enllaços o fitxers adjunts de correus falsos.
  - **Utilitza filtres de correu:** Configura el teu sistema de correu per filtrar missatges sospitosos o de remitents desconeguts.
  - **Actualitza el teu programari:** Mantingues actualitzats els sistemes operatius, aplicacions i navegadors per tancar vulnerabilitats.
- **Segrega les dades:**
  - Guarda les dades més importants en ubicacions separades i no connectades directament a Internet.
  - Limita l'accés a fitxers sensibles segons el rol de cada treballador.

Generalitat de Catalunya
SEPE
emfosi
Ajuntament de Mollet del Vallès
Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Configura controls d'accés:**
  - Implementa contrasenyes fortes i autenticació multifactor per accedir a dades i sistemes crítics.
  - Utilitza permisos per garantir que només les persones autoritzades puguin modificar o eliminar fitxers.

3.2. Importància de les còpies de seguretat en la defensa contra ransomware

Les còpies de seguretat són la millor protecció contra el ransomware, ja que et permeten restaurar els teus fitxers sense haver de pagar el rescat.

- **Estratègies per a còpies de seguretat efectives:**
  - **Regla 3-2-1:** Guarda 3 còpies de les dades, en 2 formats diferents, i almenys 1 còpia fora del lloc de treball (per exemple, al núvol).
  - **Automatitza les còpies:** Configura còpies periòdiques per assegurar-te que les dades més recents estan protegides.
  - **Aïlla les còpies de seguretat:** Utilitza sistemes que no estiguin directament connectats a la xarxa principal per evitar que el ransomware hi tingui accés.
- **Proves de recuperació:**
  - Realitza simulacions periòdiques per verificar que les còpies funcionen i que es poden restaurar ràpidament.
- **Benefici principal:**
  - En cas d'un atac, pots restaurar els fitxers sense perdre dades ni pagar el rescat.

3.3. Eines específiques per protegir-se del ransomware

Existeixen eines dissenyades per protegir el teu negoci contra el ransomware de manera proactiva.

- **Programes antivirus amb protecció contra ransomware:**
  - **Bitdefender Total Security:** Ofereix eines de detecció i prevenció específiques per al ransomware.
  - **Norton 360:** Inclou monitorització d'activitat sospitosa i protecció en temps real.
  - **Malwarebytes Premium:** Especialitzat en detectar i bloquejar programari maliciós abans que causi danys.
- **Eines de bloqueig d'execució no autoritzada:**
  - **AppLocker (Windows):** Permet bloquejar l'execució de programes no autoritzats.
- **Eines per desencriptar fitxers afectats:**
  - Si ja has estat atacat, serveis com **No More Ransom** (www.nomoreransom.org) ofereixen eines gratuïtes per desencriptar fitxers segrestats per ransomware conegut.

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

3.4. Beneficis d'aquestes estratègies

- **Continuïtat del negoci:** Les còpies de seguretat i les eines de protecció asseguren que el negoci pugui operar fins i tot després d'un atac.
- **Reducció de pèrdues:** Minimitzes el risc de perdre dades valuoses o pagar rescats costosos.
- **Tranquil·litat:** Estar preparat redueix l'estrès i et dona confiança per fer front a possibles amenaces.

4. Resiliència i resposta en cas d'incident

Tot i les millors mesures de prevenció, cap sistema és completament immune als atacs. Saber com actuar davant d'una infecció per malware o ransomware pot marcar la diferència entre una ràpida recuperació i conseqüències devastadores.

4.1. Passos a seguir si detectes una infecció

Quan sospites o detectes una infecció per malware o ransomware, és important actuar immediatament per limitar els danys.

1. **Aïlla el dispositiu afectat:**
   - Desconnecta'l de la xarxa Wi-Fi o per cable per evitar que la infecció es propagui a altres dispositius.
   - Si estàs en una xarxa d'empresa, avisa l'administrador de sistemes.
2. **No apaguis el dispositiu:**
   - Tot i que pot ser temptador, apagar el dispositiu pot dificultar la investigació i la recuperació posterior.
3. **Realitza una exploració amb un antivirus o antimalware:**
   - Utilitza programes com **Malwarebytes** o l'antivirus que tinguis instal·lat per identificar i eliminar el programari maliciós.
4. **Identifica el tipus de malware:**
   - Si es tracta d'un ransomware, intenta identificar-ne la variant per buscar eines de desencriptació (per exemple, a **No More Ransom**).
5. **Desactiva funcions d'autoexecució:**
   - Evita que el malware s'executi automàticament quan reiniciïs el sistema.

Generalitat de Catalunya
SEPE
emfosi
Ajuntament de Mollet del Vallès
Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

4.2. Com gestionar un atac de ransomware sense pagar rescats

El pagament del rescat no garanteix la recuperació de les dades i només incentiva els ciberdelinqüents a continuar els seus atacs. En lloc de pagar, segueix aquests passos:

Avaluació inicial:

- Determina quins fitxers han estat xifrats i si hi ha còpies de seguretat disponibles.

Busca eines de desencriptació:

- Plataformes com **No More Ransom** ofereixen eines gratuïtes per desbloquejar fitxers afectats per variants conegudes de ransomware.

Restaura les dades des de còpies de seguretat:

- Si tens còpies aïllades i no afectades, restaura els fitxers després d'eliminar el ransomware.

Assegura el sistema:

- Un cop eliminada la infecció, reforça les mesures de seguretat abans de reconnectar el dispositiu a la xarxa.

Aprèn de l'incident:

- Analitza com s'ha produït l'atac i implementa millores per prevenir futurs incidents (per exemple, millorar les pràctiques de seguretat del correu electrònic o limitar els permisos d'accés).

4.3. Contactar amb professionals o autoritats en casos d'atac

Hi ha situacions en què és necessari demanar ajuda externa per gestionar l'incident.

- **Contacta amb professionals de ciberseguretat si:**
  - La infecció afecta diversos dispositius o xarxes.
  - Les dades afectades són crítiques i no tens còpies de seguretat accessibles.
  - No estàs segur de com eliminar el malware o protegir el sistema.
- **Informa les autoritats si:**

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- Es tracta d'un atac de ransomware que afecta dades personals de clients o treballadors (obligació legal segons el RGPD).
- Has rebut amenaces o intents d'extorsió per part dels atacants.
- Vols contribuir a la investigació d'atacs similars.

- **Punts de contacte recomanats:**
  - **INCIBE (Institut Nacional de Ciberseguretat):** Telèfon gratuït d'ajuda (017) disponible per a empreses i particulars.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

  - **Agència de Ciberseguretat de Catalunya (CATALONIA-CERT):** Suport especialitzat en incidents de seguretat a la regió.

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Beneficis d'una resposta adequada

- **Minimització dels danys:** Actuar ràpidament redueix la propagació de la infecció i el temps d'interrupció.
- **Protecció de la reputació:** Una resposta clara i professional ajuda a mantenir la confiança dels clients i col·laboradors.
- **Aprenentatge per al futur:** Les lliçons apreses d'un incident milloren la seguretat i la resiliència del teu negoci.

5. Eines per protegir el teu negoci

Hi ha moltes eines disponibles al mercat per protegir-te contra malware i ransomware, i cada negoci té necessitats diferents. Aquesta secció **proporciona algunes opcions conegudes, però tingues en compte que la tecnologia evoluciona constantment**, i aquestes eines poden tenir versions gratuïtes, de pagament o amb funcionalitats addicionals que cal contractar a part.

Nota important: Les eines llistades en aquesta guia són exemples representatius i no les úniques opcions. T'invitem a explorar alternatives que s'ajustin millor al teu negoci, pressupost i necessitats de projecte de negoci.

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

5.1. Antivirus i antimalware per a petites empreses

Els antivirus són el punt de partida per protegir els dispositius del teu negoci contra malware. La seva funció principal és detectar i eliminar programari maliciós abans que causi problemes.

- **Exemples d'eines populars:**
  - **Bitdefender:** Inclou protecció avançada contra ransomware i eines d'optimització del sistema.
  - **Norton:** Ofereix protecció antivirus juntament amb funcionalitats com VPN integrada.
  - **Malwarebytes:** Fàcil d'utilitzar i especialitzat en eliminar malware.
  - **Avast:** Solució amb funcions bàsiques gratuïtes i opcions de pagament per a necessitats avançades.
- **Consells pràctics:**
  - Mantingues l'antivirus sempre actualitzat.
  - Realitza escaneigs regulars dels dispositius i mitjans externs.
  - Configura alertes per detectar comportaments sospitosos.

5.2. Tallafocs, VPNs i algunes eines per supervisar la xarxa

Aquestes eines ajuden a protegir la teva connexió a Internet i a detectar possibles problemes abans que es converteixin en amenaces.

- **Tallafocs:**
  - Els tallafocs actuen com a guardes entre la teva xarxa i Internet. Bloquegen connexions no autoritzades i protegeixen contra intrusions.
  - **Exemples comuns:**
    - Els tallafocs inclosos en **Windows** o **macOS**, suficients per a molts negocis petits.
    - Opcions més avançades com **pfSense** o **SonicWall**, útils per xarxes més complexes.
- **VPN (Xarxa Privada Virtual):**
  - Les VPNs xifren la connexió, protegint dades sensibles, especialment en xarxes públiques.
  - **Opcions a considerar:**
    - **NordVPN**: Per a equips que treballen remotament.
    - **ProtonVPN**: Una opció amb funcionalitats gratuïtes.
    - **ExpressVPN**: Alta velocitat i facilitat d'ús.
- **Eines de supervisió de xarxes:**
  - Permeten detectar dispositius no autoritzats o activitats sospitoses a la teva xarxa.
  - **Exemples senzills:** Solucions gratuïtes com **Zabbix** o eines professionals com **PRTG Network Monitor**.

Generalitat de Catalunya
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL SEPE
emfosi
Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

Consells generals sobre eines de protecció

1. **Investiga i compara opcions:** Tria una solució que s'ajusti a les teves necessitats i pressupost.
2. **Prova versions gratuïtes:** Algunes eines ofereixen proves gratuïtes per ajudar-te a decidir si són adequades per al teu negoci.
3. **Forma't en l'ús de les eines:** Assegura't de conèixer les funcions principals i com treure el màxim profit de cada eina.

Beneficis de tenir les eines adequades

- **Seguretat reforçada:** Redueixes el risc d'infeccions i atacs.
- **Protecció personalitzada:** Adaptes les eines a les necessitats específiques del teu negoci.
- **Tranquil·litat:** Amb les eines configurades, pots centrar-te en el teu negoci sabent que estàs protegit tot i que sempre és recomanable mantenir-se en alerta.

Aquestes eines són una base per protegir el teu negoci, però recorda mantenir-te al dia amb les noves solucions i actualitzacions tecnològiques.

6. Navegació en Xarxes Públiques o Desconegudes

A més de les eines tecnològiques, les bones pràctiques i l'educació són fonamentals per evitar infeccions per malware i ransomware. Aquest apartat descriu mesures preventives senzilles que pots implementar al teu negoci.

6.1. Educació i formació dels treballadors per evitar infeccions

Els errors humans són una de les principals causes d'infeccions per malware. Formar els treballadors (o a tu mateix si ets autònom) pot prevenir molts problemes.

- **Temes clau de formació:**
  1. **Reconèixer correus sospitosos:**
     - Correus amb errors gramaticals, remitents desconeguts o enllaços estranys.
     - Mai descarreguis fitxers adjunts no sol·licitats.
  2. **Bones pràctiques en la creació de contrasenyes:**
     - Utilitza contrasenyes llargues i úniques, preferiblement gestionades amb un gestor de contrasenyes.
  3. **Evitar accions de risc:**

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfo si · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

    - No facis clic en enllaços enviats per fonts desconegudes.
    - Evita baixar programari o fitxers d'orígens no fiables.
- **Com formar els treballadors:**
    - **Tallers o formacions en línia:** Utilitza recursos de plataformes com l'INCIBE o l'Agència de Ciberseguretat de Catalunya.
    - **Guies visuals o recordatoris:** Crea infografies senzilles amb consells pràctics que puguin consultar fàcilment.

6.2. Com protegir els dispositius en xarxes públiques o compartides

Les xarxes públiques o compartides són un punt d'entrada freqüent per als atacants. Protegir els teus dispositius en aquests entorns és essencial.

- **Evita connectar-te a xarxes públiques no segures:**
    - Només utilitza xarxes Wi-Fi protegides amb contrasenya.
    - Si és imprescindible utilitzar una xarxa pública, activa una **VPN** per xifrar la connexió.
- **Configura els dispositius adequadament:**
    - Desactiva la connexió automàtica a xarxes Wi-Fi desconegudes.
    - Activa opcions de **bloqueig automàtic** del dispositiu quan no està en ús.
    - Utilitza tallafocs i antivirus per protegir el trànsit de dades.
- **Protegeix dispositius compartits:**
    - Si diversos treballadors utilitzen el mateix dispositiu, crea comptes d'usuari separats amb permisos limitats.
    - Assegura't que cada compte estigui protegit amb contrasenyes fortes.

6.3. Bones pràctiques de gestió de correus electrònics i descàrregues

El correu electrònic és un dels canals més utilitzats pels atacants per distribuir malware i ransomware. Seguir bones pràctiques pot reduir significativament els riscos.

- **Gestió de correus electrònics:**
    - **Evita fer clic en enllaços desconeguts:** Si no confies en l'emissor, no interactuïs amb el correu.
    - **No obris fitxers adjunts sospitosos:** Desconfia especialment de formats com .exe, .zip o .bat.
    - **Configura filtres de correu brossa:** Això ajuda a evitar que correus maliciosos arribin a la safata d'entrada.
- **Descàrregues segures:**
    - Només descarrega programes i fitxers de llocs oficials o de confiança.
    - Utilitza antivirus per escanejar els fitxers abans d'obrir-los.
    - Desconfia de llocs que ofereixen programes de pagament de manera gratuïta.

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

- **Supervisa l'ús del correu electrònic:**
  - Configura sistemes per monitoritzar correus sospitosos a nivell d'empresa.
  - Forma't en la detecció de tècniques de phishing (per exemple, correus que simulen ser d'entitats bancàries o administratives).

Beneficis de les mesures preventives

- **Reducció de riscos:** Prevenir és més efectiu i econòmic que solucionar els efectes d'una infecció.
- **Protecció col·lectiva:** Una formació adequada millora la seguretat de tot el negoci.
- **Tranquil·litat:** Amb bones pràctiques, redueixes les probabilitats d'incidents i et prepares per gestionar possibles amenaces.

Aquestes mesures complementen les eines tecnològiques i reforcen la seguretat del teu negoci.

7. Preguntes d'autoavaluació

L'autoavaluació és un pas fonamental per determinar el nivell de protecció del teu negoci contra el malware i ransomware. Aquesta secció inclou una llista de verificació i recomanacions personalitzades per ajudar-te a identificar àrees de millora.

7.1. Llista de verificació (Checklist dels conceptes principals)

Respon les següents preguntes amb **Sí** o **No**. Si la resposta és "No" a alguna d'elles, revisa l'apartat corresponent de la guia per implementar les millores necessàries.

Antivirus i antimalware

1. Tinc instal·lat un antivirus actualitzat en tots els dispositius del negoci?
2. Realitzo escaneigs periòdics amb un antivirus o antimalware?
3. He configurat alertes per detectar activitats sospitoses en temps real?

Còpies de seguretat i restauració

4. Realitzo còpies de seguretat regulars seguint la regla 3-2-1?
5. Les còpies de seguretat estan aïllades per evitar que el ransomware les afecti?
6. He provat recentment la restauració de les còpies de seguretat per garantir-ne la funcionalitat?

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

Gestió de correus electrònics i descàrregues

7. Sempre verifico l'autenticitat dels correus electrònics abans d'obrir-los?
8. Només descarrego fitxers i aplicacions de fonts oficials i confiables?
9. He configurat filtres de correu brossa per evitar missatges maliciosos?

Protecció de xarxes i dispositius

10. Utilitzo una VPN per protegir les connexions en xarxes públiques o compartides?
11. Els dispositius del negoci estan configurats amb tallafocs actius?
12. He desactivat la connexió automàtica a xarxes Wi-Fi no segures?

Formació i conscienciació

13. Jo i/o el meu equip hem rebut formació sobre ciberseguretat bàsica?
14. Conec les tècniques habituals de phishing i com evitar-les?

7.2. Resultats i Recomanacions

0-5 respostes afirmatives: Nivell de risc alt
• Estàs molt exposat a infeccions per malware i ransomware. • Recomanació: Prioritza les accions bàsiques, com instal·lar un antivirus, configurar còpies de seguretat i educar-te en detecció d'amenaces.
6-10 respostes afirmatives: Nivell de risc moderat
• Tens algunes mesures implementades, però encara hi ha vulnerabilitats importants. • Recomanació: Dona prioritat a protegir les teves xarxes, millorar la gestió de correus electrònics i assegurar les còpies de seguretat.
11-13 Respostes afirmatives: Nivell de risc baix
• Tens una estratègia de seguretat robusta, però pots millorar alguns detalls. • Recomanació: Revisa la configuració dels teus dispositius i xarxes per assegurar-te que estan totalment protegits.
14 Respostes afirmatives: Excel·lent
• Felicitats! Tens un alt nivell de protecció contra malware i ransomware. • Recomanació: Mantingues les bones pràctiques i actualitza't sobre noves eines i amenaces per mantenir aquest nivell de seguretat.

Generalitat de Catalunya
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL SEPE
emfosl
Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local

7.3. Recursos addicionals

Per reforçar la teva estratègia contra el malware i el ransomware, et recomanem consultar els recursos següents. Aquests t'ajudaran a millorar en les àrees on has detectat mancances i a mantenir-te actualitzat sobre les millors pràctiques i eines:

Guies i recursos en línia

- **INCIBE (Institut Nacional de Ciberseguretat):**
  - Ofereix guies, consells i eines gratuïtes per protegir petites empreses contra malware i ransomware.
  - Accedeix al seu lloc web: www.incibe.es.
- **Agència de Ciberseguretat de Catalunya (Catalonia-CERT):**
  - Proporciona recomanacions específiques per a negocis a Catalunya, així com eines per gestionar incidents de seguretat.
  - Web oficial: www.ciberseguretat.gencat.cat

Eines de formació en línia

- **Plataformes de formació gratuïtes:**
  - **Coursera** i **Udemy:** Ofereixen cursos introductoris en ciberseguretat.
  - **INCIBE Formació:** Programes dissenyats per a petites empreses i autònoms.
  - **Google Actívate:** Cursos gratuïts en seguretat digital i bones pràctiques.
- **Tallers locals i webinars:**
  - Estigues atent a les formacions organitzades per cambres de comerç o associacions d'empresaris a la teva regió.

Suport i assistència

- **INCIBE (017):**
  - Telèfon d'ajuda gratuït per a empreses i particulars, disponible tots els dies de l'any. Pots consultar dubtes sobre incidents de seguretat, com ara infeccions per malware o ransomware.
- **Catalonia-CERT:**
  - Contacta amb el servei regional per gestionar incidents a nivell local.
- **Suport del proveïdor de les teves eines:**
  - Si utilitzes antivirus, antimalware o eines de còpia de seguretat, molts proveïdors ofereixen assistència tècnica i recursos específics per gestionar incidents.

Aquests recursos t'ajudaran a enfortir la teva defensa contra el malware i el ransomware, i a mantenir-te informat sobre les últimes tècniques de protecció.

Generalitat de Catalunya · Ministerio de Trabajo y Economía Social SEPE · emfosi · Ajuntament de Mollet del Vallès

Aquesta acció està subvencionada pel Servei Públic d'Ocupació de Catalunya en el marc dels Programes de suport al desenvolupament local