Autoavalua la ciberseguretat del teu projecte:

Guia per protegir-te contra correus electrònics maliciosos i Phishing.

Una guia per protegir-te i autoavaluar la ciberseguretat del teu projecte o petita empresa amb recomanacions per detectar i evitar correus electrònics sospitosos i intents de phishing.

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:

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

1.1. Què és el phishing i per què és un risc per a petites empreses i autònoms

El **phishing** és una tècnica utilitzada pels ciberdelinqüents per enganyar persones perquè revelin informació sensible, com ara contrasenyes, dades bancàries o informació personal. Normalment, els atacs de phishing es presenten com a **correus electrònics falsos**, dissenyats per semblar enviats per entitats legítimes com bancs, serveis d'entrega o fins i tot institucions governamentals.

- **Com funciona el phishing?**
  - Els atacants envien un correu electrònic amb:
    - **Enllaços maliciosos:** Redirigeixen l'usuari a llocs web falsos que recullen informació.
    - **Fitxers adjunts infectats:** Quan s'obren, instal·len malware al dispositiu.
    - **Missatges d'urgència:** Frases com "Verifica el teu compte ara" o "El teu compte serà bloquejat" per generar pànic i obtenir una reacció ràpida.
- **Per què és un risc per a petits empresaris i autònoms?**
  - **Limitació de recursos:** Sovint, no tenen equips de ciberseguretat per detectar i gestionar aquests atacs.
  - **Accés directe a dades sensibles:** En molts casos, els autònoms gestionen personalment informació crítica del negoci i dels seus clients.
  - **Impacte financer i reputacional:** Un incident pot generar pèrdues econòmiques i danyar la confiança dels clients.

1.2. Impacte d'un atac de phishing o correu maliciós en un negoci petit

Els atacs de phishing poden tenir conseqüències devastadores per a petites empreses i autònoms, ja que sovint no disposen de les eines ni els recursos per fer front a les seves conseqüències.

- **Principals impactes d'un atac:**
  1. **Pèrdua d'informació:**
     - Els atacants poden obtenir accés a dades bancàries, informació de clients o contrasenyes del negoci.
  2. **Pèrdua financera:**
     - Els atacs poden suposar càrrecs fraudulents, transaccions no autoritzades o fins i tot demandes per la gestió inadequada de dades de clients.
  3. **Danys a la reputació:**

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

        - Si les dades dels clients són compromeses, pot ser difícil recuperar la seva confiança.
    4. **Temps i recursos perduts:**
        - La recuperació després d'un atac implica temps, diners i esforç per restablir sistemes, informar clients i reforçar la seguretat.
- **Exemple pràctic:**
    - Un petit negoci rep un correu suposadament del seu banc, sol·licitant verificar informació confidencial. El propietari introdueix les dades a un lloc web fals i l'atacant utilitza aquesta informació per accedir al compte bancari del negoci, retirant fons o canviant configuracions crítiques.

Objectius d'aquesta guia

Amb aquesta guia, aprendràs:

1. A reconèixer els senyals d'advertència d'un correu electrònic sospitós.
2. A gestionar correus electrònics empresarials de manera segura.
3. A protegir el teu negoci davant d'atacs de phishing i a respondre adequadament si es produeix un incident.

2. Com identificar correus electrònics sospitosos

Reconèixer un correu electrònic de phishing és essencial per evitar caure en fraus. Els correus electrònics sospitosos sovint tenen característiques comunes que els diferencien dels legítims. Aquest apartat t'ajudarà a identificar-los i protegir-te.

2.1. Característiques habituals dels correus de phishing

Els correus electrònics de phishing solen utilitzar tècniques d'engany per semblar legítims i persuadir-te perquè facis alguna acció, com clicar un enllaç o compartir informació.

- **Característiques més comunes:**
    1. **Urgència falsa:**
        - Frases com "Acció necessària immediatament" o "El teu compte serà bloquejat en 24 hores".
    2. **Enllaços sospitosos:**
        - Enllaços que semblen oficials però que dirigeixen a llocs web falsos. Per exemple, **www.elmeubaank.com** en lloc de **www.elmeubanc.com**.

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

3. **Errors ortogràfics i gramaticals:**
    - Els correus maliciosos sovint tenen errors perquè els ciberdelinqüents no sempre són experts en l'idioma.
4. **Adreça del remitent desconeguda o falsa:**
    - El correu sembla provenir d'una entitat coneguda, però l'adreça de correu electrònic no coincideix (exemple: **suport@bancosegur.xyz** en lloc de **suport@bancosegur.com**).

2.2. Errors comuns en correus maliciosos

Reconèixer certs errors freqüents pot ajudar-te a evitar accions que comprometin la seguretat.

- **Remitents falsos:**
    - Els ciberdelinqüents sovint utilitzen noms coneguts (bancs, institucions governamentals, etc.), però l'adreça del remitent no correspon amb el domini oficial.
- **Enllaços sospitosos:**
    - Passa el cursor per sobre de l'enllaç (sense clicar) per veure la URL real. Si sembla estranya, llarga o no correspon al lloc legítim, no hi facis clic.
- **Urgències falses:**
    - Els correus de phishing busquen que actuïs ràpidament sense pensar. Missatges com "Confirmació urgent requerida" són una tàctica per reduir el teu temps de reflexió.
- **Sol·licituds d'informació confidencial:**
    - Cap institució legítima sol·licita contrasenyes, dades bancàries o altres informació sensible a través d'un correu electrònic.

2.3. Exemples pràctics de correus electrònics sospitosos

A continuació, es detallen exemples comuns que pots trobar i com detectar-los:

1. **Phishing bancari:**
    - **Missatge:** "El teu compte ha estat bloquejat. Clica aquí per verificar la teva informació."
    - **Senyals de sospita:**
        - L'enllaç condueix a una pàgina que no és el web oficial del banc.
        - Hi ha errors d'ortografia en el text del correu.
        - L'adreça del remitent no coincideix amb el domini del banc.
2. **Frau en entregues de paquets:**
    - **Missatge:** "Hem intentat lliurar un paquet sense èxit. Fes clic per reprogramar l'entrega."
    - **Senyals de sospita:**

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

        - No esperaves cap paquet.
        - L'enllaç condueix a una pàgina que sol·licita dades bancàries per pagar una suposada taxa.
3. **Suport tècnic fals:**
    - **Missatge:** "Hem detectat activitat sospitosa al teu ordinador. Contacta amb el suport tècnic immediatament."
    - **Senyals de sospita:**
        - Sol·liciten instal·lar un programa de control remot.
        - L'adreça del remitent no correspon a cap proveïdor de serveis tecnològics conegut.

Consells per actuar davant d'un correu sospitós

1. No facis clic en cap enllaç ni obris fitxers adjunts.
2. Comprova l'adreça del remitent i revisa si coincideix amb el domini oficial.
3. Contacta directament amb l'entitat suposadament emissora a través de canals oficials.

Beneficis de reconèixer correus sospitosos

- **Evites filtracions de dades:** Protegeixes informació sensible personal i empresarial.
- **Redueixes riscos financers:** Evites pèrdues derivades de transaccions fraudulentes.
- **Tranquil·litat:** Tens confiança per gestionar correus electrònics amb seguretat.

3. Bones pràctiques per gestionar correus a l'empresa

La gestió segura del correu electrònic és essencial per evitar caure en atacs de phishing o rebre contingut maliciós. Amb algunes normes bàsiques, pots protegir millor el teu negoci i mantenir la confiança en les comunicacions.

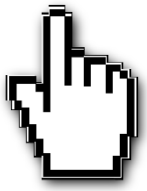
3.1. Normes per gestionar correus desconeguts o inesperats

Els correus electrònics desconeguts o inesperats poden ser una porta d'entrada per a ciberatacs. Seguir aquestes normes t'ajudarà a evitar problemes:

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

- **Revisa amb atenció el remitent:**
  - Comprova l'adreça del correu electrònic. Si no coneixes el remitent o l'adreça sembla sospitosa (per exemple, **suport@clientes-banc.xyz**), no obris el missatge.
- **Evita obrir fitxers adjunts:**
  - No obris fitxers adjunts d'orígens desconeguts o inesperats, especialment si són formats com **.exe**, **.zip** o **.bat**, ja que podrien contenir malware.
- **No responguis al correu:**
  - Respondràs a una possible adreça maliciosa, confirmant que el teu correu electrònic està actiu.
- **Confirma amb el remitent legítim:**
  - Si tens dubtes, contacta amb l'entitat suposadament emissora a través del seu canal oficial (per exemple, el web oficial o un número de telèfon verificat).

3.2. Com comprovar la seguretat dels remitents i enllaços



Els correus sospitosos sovint inclouen remitents falsos i enllaços dissenyats per semblar legítims. Aquí tens algunes tècniques per comprovar la seva autenticitat:

- **Comprova l'adreça del remitent:**
  - Compara l'adreça del correu amb el domini oficial de l'empresa. Per exemple:
    - Correcte: **info@bancosegur.com**
    - Sospitós: **info@bancosegur.xyz**
- **Revisa els enllaços abans de clicar-hi:**
  - Passa el cursor per sobre de l'enllaç (sense fer-hi clic) per veure la URL completa. Si la URL sembla estranya, llarga o no coincideix amb l'empresa legítima, no hi facis clic.
- **Utilitza eines per analitzar enllaços:**
  - Plataformes com **VirusTotal** poden ajudar-te a verificar si un enllaç és segur abans de clicar-hi.

3.3. Consells per evitar clics accidentals en contingut maliciós

És fàcil caure en l'error de clicar un enllaç o obrir un fitxer sense voler. Per evitar-ho, segueix aquests consells:

- **Pren-t'ho amb calma:**
  - Els correus maliciosos sovint utilitzen un llenguatge urgent per pressionar-te. Llegeix el missatge amb atenció abans d'actuar.
- **Evita clicar enllaços dins del correu:**
  - Si creus que l'enllaç és legítim, accedeix manualment al lloc web escrivint l'adreça al navegador.
- **Configura filtres automàtics:**

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

  - Activa filtres de correu brossa al teu proveïdor de correu electrònic per reduir la quantitat de correus sospitosos que arriben a la safata d'entrada.
- **Utilitza una solució de seguretat per al correu:**
  - Antivirus i solucions com **Microsoft Defender for Office 365** o **Google Workspace Security** poden analitzar i bloquejar contingut maliciós abans que arribi a la teva safata d'entrada.

Beneficis d'aquestes bones pràctiques

- **Protecció millorada:** Redueixes el risc de caure en trampes de phishing o d'exposar dades sensibles.
- **Eficiència i tranquil·litat:** Gestionar els correus amb seguretat et permet centrar-te en les tasques importants sense preocupacions.
- **Imatge professional:** Mantenir un control adequat dels correus electrònics empresarials reforça la confiança dels teus clients i col·laboradors.

4. Eines i configuracions per protegir-te del phishing

Disposar de les eines adequades i configurar-les correctament és fonamental per prevenir atacs de phishing. Aquest apartat inclou solucions senzilles i pràctiques que pots utilitzar per protegir-te.

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.

4.1. Filtres de correu brossa i eines de seguretat integrades

Els filtres de correu brossa i les funcions de seguretat integrades als proveïdors de correu electrònic són una defensa bàsica contra el phishing.

- **Activa els filtres de correu brossa:**
  - La majoria de proveïdors, com **Gmail**, **Outlook** o **Yahoo Mail**, tenen filtres automàtics per detectar correus sospitosos.
  - **Com activar-los:**
    - **Gmail:** Configuració > Filtres i adreces bloquejades > Crea un nou filtre per enviar correus sospitosos a la carpeta de correu brossa.
    - **Outlook:** Configuració > Correu > Correu no desitjat > Activa filtres de correu brossa avançats.
- **Revisa la carpeta de correu brossa:**

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

- Encara que els filtres són útils, de tant en tant revisa la carpeta de correu brossa per assegurar-te que no hi ha missatges legítims marcats per error.

- **Eines integrades de seguretat:**
  - Alguns serveis, com Google Workspace o Microsoft 365, ofereixen funcions avançades per analitzar i bloquejar correus sospitosos abans que arribin a la safata d'entrada.

4.2. Extensions de navegadors i aplicacions per identificar amenaces

Els navegadors i aplicacions de seguretat poden ajudar-te a identificar i evitar enllaços sospitosos o pàgines web malicioses.

- **Com instal·lar extensions al navegador:**
  - Per a **Chrome:** Accedeix al Chrome Web Store, cerca l'extensió desitjada i fes clic a "Afegeix al navegador".
  - Per a **Firefox:** Ves a **Complementos** > Cerca l'extensió i fes clic a "Afegeix a Firefox".

4.3. Com configurar alertes de seguretat en correus electrònics

Molts proveïdors de correu electrònic permeten configurar alertes de seguretat per advertir-te sobre correus sospitosos.

- **Activa les alertes integrades:**
  - **Gmail:** Els correus sospitosos es marquen automàticament amb una advertència, com "Aquest missatge podria ser un intent de phishing".
  - **Outlook:** Activa les opcions de "Missatges sospitosos" perquè els correus es redirigeixin automàticament a la carpeta de correu no desitjat.
- **Configura filtres personalitzats:**
  - Crea filtres per detectar paraules o frases típiques de phishing, com "Urgent" o "Verifica ara", i redirigir aquests correus a una carpeta específica.
- **Configura notificacions al mòbil:**
  - Activa les notificacions per a correus sospitosos o bloquejats en aplicacions com Gmail o Outlook per estar al corrent dels intents d'atac.

Beneficis d'utilitzar eines i configuracions de seguretat

- **Protecció automàtica:** Les eines treballen en segon pla per detectar i bloquejar correus sospitosos.
- **Reducció del risc d'errors humans:** Les alertes i filtres ajuden a prevenir clics accidentals.

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

- **Tranquil·litat:** Pots gestionar correus electrònics amb més seguretat, sabent que tens una capa extra de protecció.

5. Gestió de dades i seguretat en cas d'un atac de phishing

Si caus en un atac de phishing, és crucial actuar ràpidament per minimitzar l'impacte i protegir el teu negoci. Aquest apartat explica què fer immediatament després de clicar en un enllaç sospitós, com recuperar el control si les dades han estat compromeses i com evitar futurs incidents.

5.1. Què fer si has clicat en un enllaç sospitós

Si accidentalment has clicat en un enllaç sospitós, segueix aquests passos immediatament per protegir-te:

1. **No introdueixis cap dada personal:**
   - Si l'enllaç t'ha portat a una pàgina que sol·licita informació (com contrasenyes o dades bancàries), no hi introdueixis res.
2. **Tancla la pàgina web immediatament:**
   - No interactuïs amb cap contingut de la pàgina. Si has descarregat algun fitxer, no l'obris.
3. **Desconnecta't d'Internet:**
   - Si sospites que el dispositiu podria estar compromès, desactiva la connexió Wi-Fi o de dades mòbils per evitar més transmissions.
4. **Escaneja el dispositiu amb un antivirus:**
   - Utilitza un programa de seguretat per escanejar el dispositiu i detectar possibles infeccions.

5.2. Com recuperar el control si les teves dades han estat compromeses

Si les teves dades ja han estat compromeses, actua immediatament per limitar els danys.

1. **Canvia les contrasenyes afectades:**
   - Si has compartit credencials, canvia immediatament la contrasenya dels comptes afectats. Assegura't que sigui única i robusta.
2. **Activa l'autenticació multifactor (MFA):**
   - Afegeix una capa de seguretat als teus comptes mitjançant MFA (per exemple, verificació amb codi SMS o aplicacions com Google Authenticator).
3. **Informa els proveïdors afectats:**

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

   - Si has compartit dades bancàries, contacta amb el teu banc per bloquejar targetes o comptes, si és necessari.
   - Notifica qualsevol pèrdua d'informació a serveis rellevants, com el teu proveïdor de correu electrònic.
4. **Monitoritza activitat sospitosa:**
   - Revisa els teus comptes per detectar transaccions no autoritzades o accessos estranys.
5. **Informa les autoritats:**
   - Si les dades robades inclouen informació personal sensible o financera, considera presentar una denúncia. A Catalunya, pots contactar amb el **Catalonia-CERT**.

5.3. Bones pràctiques per protegir-te després d'un incident

Un cop hagis gestionat un atac de phishing, és important reforçar les teves defenses per evitar futurs incidents.

- **Educa't i educa l'equip:**
  - Repassa els senyals d'un correu sospitós i assegura't que tots els col·laboradors del negoci entenen com identificar-los.
- **Revisa les configuracions de seguretat:**
  - Activa filtres de correu brossa més estrictes i assegura't que les eines de seguretat estan configurades adequadament.
- **Implementa un gestor de contrasenyes:**
  - Utilitza eines per gestionar i protegir les contrasenyes.
- **Fes còpies de seguretat regulars:**
  - Assegura't que les dades crítiques estan protegides i poden ser restaurades fàcilment si cal.
- **Actualitza les eines i sistemes:**
  - Mantingues actualitzats els sistemes operatius, navegadors i aplicacions per protegir-te contra vulnerabilitats.

Beneficis de respondre adequadament a un atac

- **Minimització de danys:** Actuar ràpidament redueix l'impacte d'un atac i protegeix informació valuosa.
- **Confiança restaurada:** Reforçar la seguretat després d'un incident demostra compromís amb la protecció de dades.
- **Preparació futura:** Amb les mesures adequades, estaràs millor preparat per identificar i gestionar futurs intents de phishing.

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

6. Preguntes d'auoavaluació.

Aquest apartat et permet valorar el nivell de seguretat en la gestió dels teus correus electrònics. Amb una llista de verificació i recomanacions, podràs identificar punts de millora per protegir-te contra el phishing i correus maliciosos.

6.1. 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.

Identificació de correus sospitosos

1. Reviso amb atenció l'adreça del remitent abans d'obrir un correu electrònic?
2. Passo el cursor per sobre dels enllaços per verificar la URL abans de clicar-hi?
3. Evito obrir fitxers adjunts de correus desconeguts o inesperats?

Gestió de correus electrònics

4. Utilitzo filtres de correu brossa per reduir l'arribada de missatges sospitosos?
5. Reviso regularment la carpeta de correu brossa per assegurar-me que no hi ha correus legítims bloquejats?
6. No responc mai a correus sospitosos que sol·liciten informació personal o professional?

Protecció contra el phishing

7. Tinc instal·lades extensions o aplicacions per analitzar correus electrònics i detectar amenaces?
8. Configuro alertes de seguretat per advertir-me de correus sospitosos o no segurs?

Gestió de dades i actuació en incidents

9. Sé què fer si clico en un enllaç sospitós (per exemple, desconnectar-me d'Internet i escanejar el dispositiu)?
10. Canvio immediatament les contrasenyes si crec que han estat compromeses?
11. Activo l'autenticació multifactor (MFA) als comptes importants per protegir-me d'accessos no autoritzats?

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

Escala d'autoavaluació

0-3 respostes afirmatives: Nivell de risc alt
• Estàs molt exposat a riscos relacionats amb el phishing i correus maliciosos. • Recomanació: Prioritza la configuració de filtres de correu brossa, l'ús d'eines de seguretat i la formació sobre com identificar correus sospitosos.
4-7 respostes afirmatives: Nivell de risc moderat
• Tens algunes mesures implementades, però encara hi ha vulnerabilitats significatives. • Recomanació: Reforça l'ús d'eines de seguretat avançades, millora la gestió de correus sospitosos i assegura't de saber com actuar en cas d'incident.
8-10 respostes afirmatives: Nivell de risc baix
• Tens una bona estratègia de seguretat en marxa, però pots millorar certs detalls. • Recomanació: Revisa les configuracions de seguretat periòdicament i fes formacions periòdiques per mantenir les teves habilitats actualitzades.
11 respostes afirmatives: Excel·lent
• Felicitats! La teva gestió de correus electrònics és segura i efectiva. • Recomanació: Mantingues les bones pràctiques, actualitza regularment les eines de seguretat i adapta les mesures segons noves necessitats o amenaces.

Recursos addicionals

Per reforçar la teva estratègia en la protecció contra correus electrònics maliciosos i phishing, et recomanem consultar els recursos següents. Aquests t'ajudaran a millorar la teva defensa contra aquests atacs i a mantenir-te actualitzat sobre les millors pràctiques en seguretat del correu electrònic.

Eines de formació en línia

- **Plataformes de formació gratuïtes:**
  - **INCIBE Formació:** Programes dissenyats per ajudar petites empreses a identificar i evitar correus electrònics maliciosos.
  - **Google Actívate:** Ofereix cursos gratuïts en seguretat digital i bones pràctiques de gestió de correus electrònics.
- **Tallers locals i webinars:**
  - Cambres de comerç i associacions empresarials sovint organitzen formacions específiques en seguretat del correu electrònic i prevenció de phishing.

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

Suport i assistència

- **INCIBE (017):**
  - Telèfon d'ajuda gratuït disponible tots els dies de l'any, amb assessorament per a empreses i particulars sobre incidents de phishing i seguretat en correus electrònics.
  - Web oficial: www.incibe.es.
- **Catalonia-CERT (Agència de Ciberseguretat de Catalunya):**
  - Ofereix suport tècnic i assessorament específic per a petites empreses en casos d'incidents relacionats amb correus electrònics sospitosos o compromesos.
  - Web oficial: www.ciberseguretat.gencat.cat.
- **Suport dels proveïdors de correu electrònic:**
  - **Gmail:** Ofereix eines per reportar phishing i configurar filtres de seguretat.
    Accés: support.google.com.
  - **Outlook:** Proporciona assistència tècnica per gestionar correus sospitosos i millorar la configuració de seguretat.
    Accés: support.microsoft.com.

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