



Prevención de estafas en el ámbito empresarial: cómo evitar el BEC

COMISARÍA PROVINCIAL DE CÓRDOBA

Grupo IV Brigada Provincial de Policía Judicial (NN.TT. II)

Delegación de Participación Ciudadana

WHOAMI

- **Root:~#**

Karim M. Laamrani.

- ❑ INSPECTOR DE POLICÍA, JEFE DEL GRUPO IV DE LA BPPJ (NN.TT. II)
- ❑ CURSO DE DELITOS TECNOLÓGICOS DE @POLICIA
- ❑ EL MUNDO CIBER COMO FUTURO



@KURTUBA3110

- **www-data:~#**

Miguel A. Agredano.

- ❑ POLICÍA INVESTIGADOR DEL GRUPO IV DE LA BPPJ.
- ❑ ETERNO APRENDIZ
- ❑ APASIONADO DE LA CIBERSEGURIDAD.



@Txicoagredano

GUÍA



Introducción



**Modalidades estafas
tipo BEC**



Medidas de prevención



Conclusiones



Preguntas

JUSTIFICACIÓN

- Aumento de las estafas tipo BEC
- Gran perjuicio económico
- Viabilidad PYMES

MODALIDADES

- Man in the Middle
- Fraude del CEO
- Ataques homográficos
- Robo de datos

PREVENCIÓN



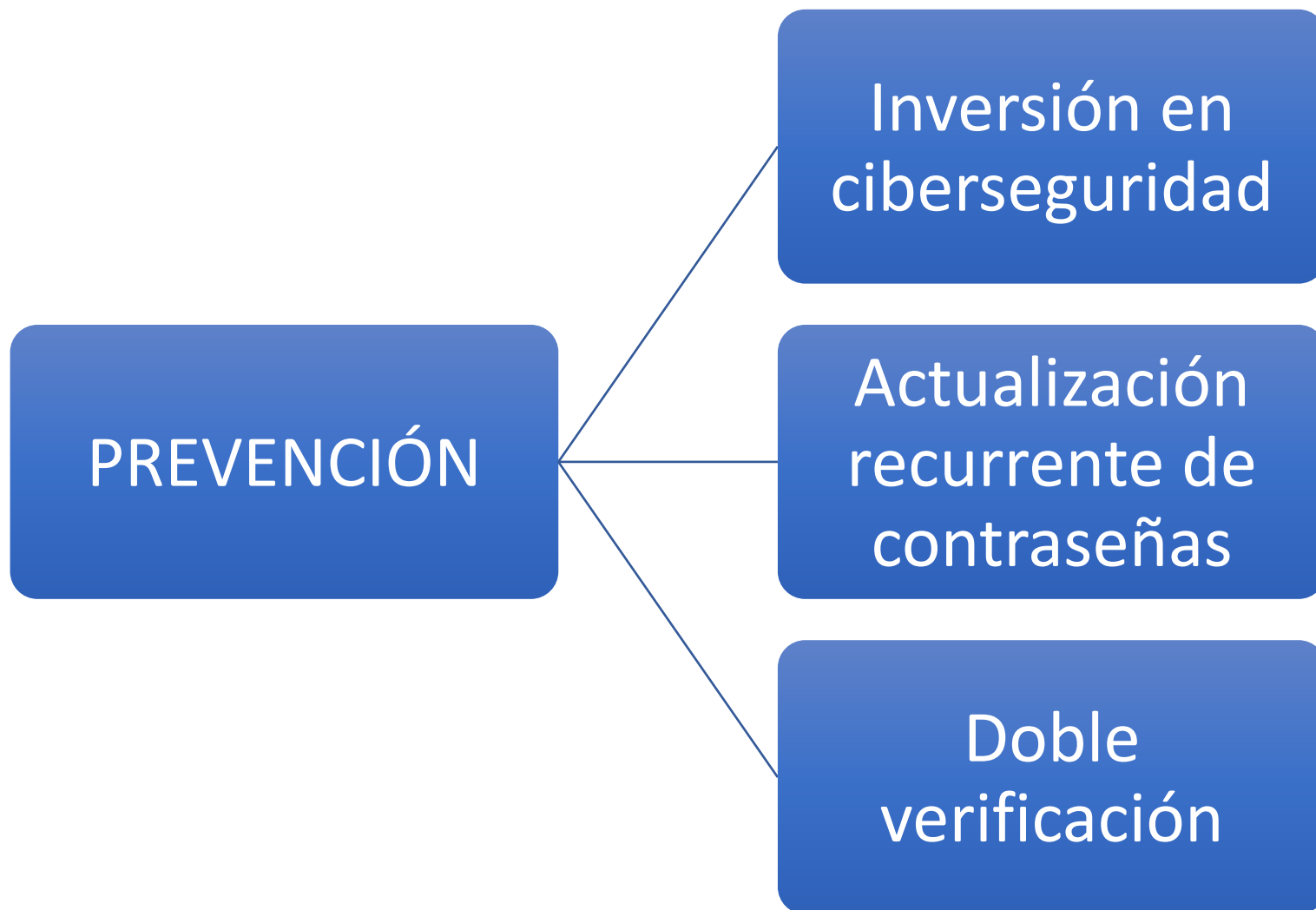
Amenazas



Vulnerabilidades



RIESGOS



PREVENCIÓN NIVEL TÉCNICO

Las medidas de ciberseguridad son una inversión, no un gasto



AMENAZA+VULNERABILIDAD =
RIESGO

PREVENCIÓN NIVEL TÉCNICO

- No basta con medidas tecnológicas (IDS, IPS, CORTAFUEGOS...) y fin del problema



- Es necesario tener una CONCIENCIACIÓN-FORMACIÓN para empleados que aborde los posibles riesgos.

PREVENCIÓN NIVEL TÉCNICO

- Tener instaladas las últimas actualizaciones en los dispositivos.

 **2008**

CVE-2008-3844  **9.3** Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

 **2007**

CVE-2007-2768  **4.3** OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

<https://www.shodan.io/host/92.204.211.238>

PREVENCIÓN NIVEL TÉCNICO

- Tener un hosting dedicado en la medida de lo posible vs un hosting compartido



PREVENCIÓN NIVEL TÉCNICO

- Políticas de SPF y DMARC bien definidas, evitar que correos electrónicos fraudulentos o *spoofeados* entren a la bandeja de entrada.

5 Problems

Category	Host	Result	
dmARC	newegylooktours.com	DMARC Quarantine/Reject policy not enabled	More Info
smtp	mx-biz.mail.am0.yahoodns.net	May be an open relay.	More Info
smtp	mx-biz.mail.am0.yahoodns.net	May be an open relay.	More Info
mx	newegylooktours.com	DMARC Quarantine/Reject policy not enabled	More Info
smtp	mx-biz.mail.am0.yahoodns.net	May be an open relay.	More Info

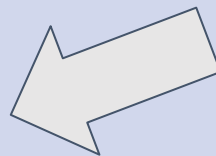
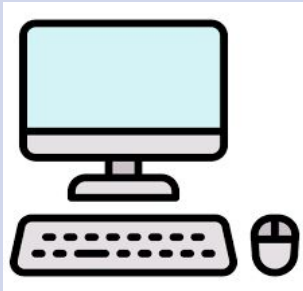
<https://mxtoolbox.com/emailhealth/newegylooktours.com/>

PREVENCIÓN NIVEL TÉCNICO

- VULNERABILIDAD “OPEN RELAY”. Permite modificar X-Sender y poner cualquier dirección de correo electrónico.

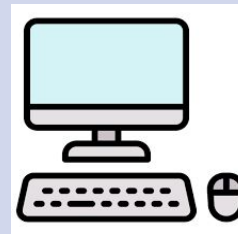
correo@miempresa.com

dirección original

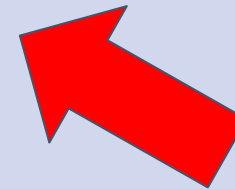


X-Sender modificado
como

correo@proveedor.com



servidor con
vulnerabilidad “OPEN
RELAY”

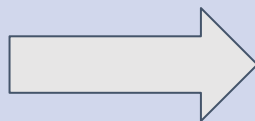


PREVENCIÓN NIVEL TÉCNICO

- Registro y compra de dominios parecidos con TLD diferente.

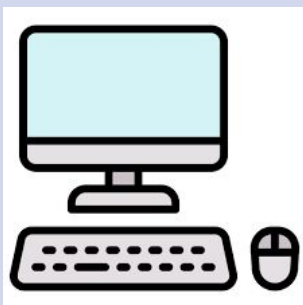
correo@miempresa.com

dirección original



correo@miempresa.co

dirección spoofeada

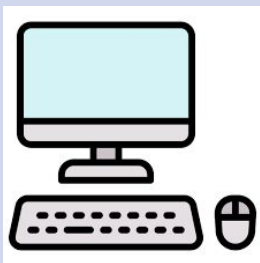


PREVENCIÓN NIVEL TÉCNICO

- Atención con el campo “Reply-to” (Responder).

correo@miempresa.com

dirección original

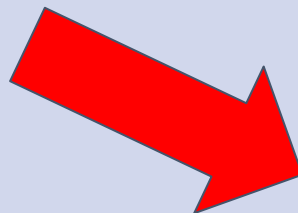
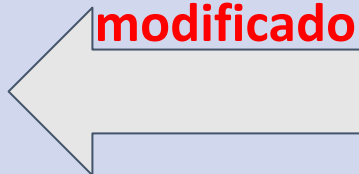


correo@proveedor.com

dirección original



“Reply to”
modificado



correo@proveedor.sl
dirección spoofeada

ATAQUES HOMOGRAFICOS

@policia

@policia

www.rnicasa.com

www.micasa.com

apple.com

apple.com

POTOSL.COM

POTOSI.COM

PREVENCIÓN NIVEL TÉCNICO

- Evitar el uso de programas de *crackeo* de software ya que pueden contener en su interior “*infostealers*” y “*backdoors*”



PREVENCIÓN NIVEL TÉCNICO

- Cambio con regularidad de credenciales de correo electrónico y aplicativos.

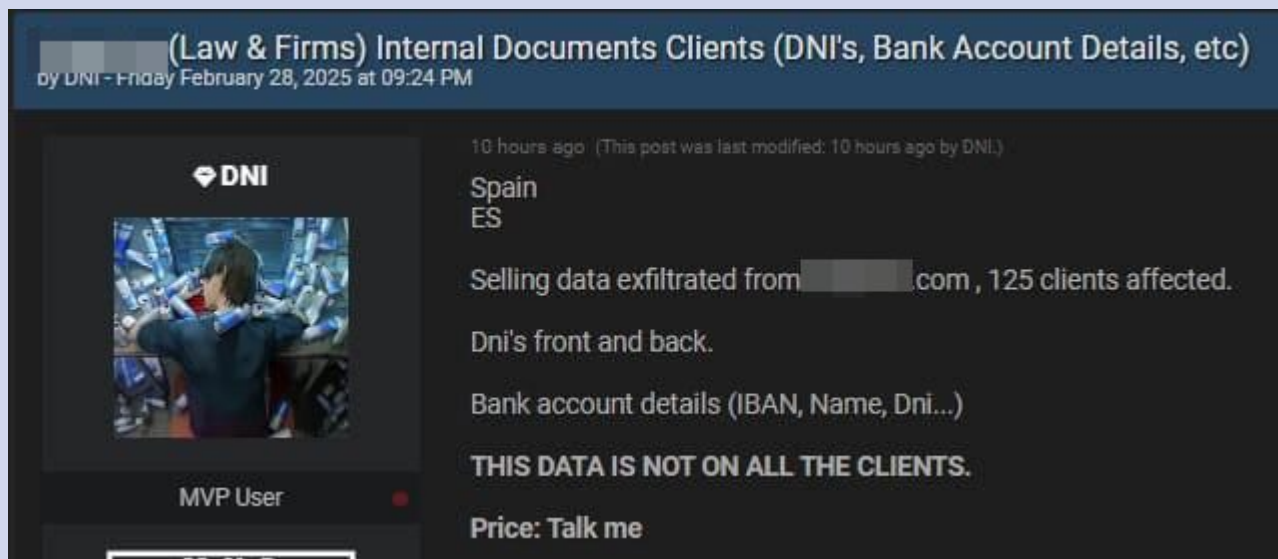
**Apoyarse en el uso de
gestores de contraseñas.**

<https://keepass.info/download.html>



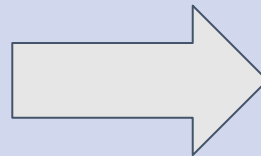
PREVENCIÓN NIVEL TÉCNICO

- DONDE ACABAN LAS CREDENCIALES?...



PREVENCIÓN NIVEL TÉCNICO

- SI SE RECIBE UN CORREO CON CAMBIO DE IBAN O MÍNIMA SOSPECHA DE ALGO...



EVITA EL 99,9% DE LOS
BUSINESS EMAIL
COMPROMISE.

HE SUFRIDO UN BEC, ¿AHORA QUÉ?



CONTACTO CON ENTIDAD BANCARIA

INTERPOSICIÓN DENUNCIA

SALVAGUARDA CORREOS ELECTRÓNICOS

CAMBIO CONTRASEÑAS

INFORME PERICIAL DE PARTE

PREVENCIÓN NIVEL TÉCNICO

- NO BORRAR EMAILS Y GUARDARLOS EN FORMATO (EML).
- NO CERRAR CONTACTO CON LOS CIBERDELINCIENTES.



CONCLUSIONES

- PREVENCIÓN
- PREVENCIÓN
- PREVENCIÓN



Grupo IV Brigada Provincial de Policía Judicial de Córdoba
Nuevas Tecnologías II (Delitos cibereconómicos)

Teléfonos: 957594652/4680

Email: cordoba.bppjtecnologicos@policia.es



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR

DIRE
DE L