CÓMO HACER TU VIDA DIGITAL MÁS SEGURA

ENTENDER EL NUEVO MUNDO

- Desde 2020 los robos de identidad y las estafas virtuales se multiplicaron exponencialmente (entre el 200% y el 3000%).
- Muchas bases de datos fueron robadas y vendidas, haciendo que las estafas sean más personalizadas.

ENTENDER EL NUEVO MUNDO

- El incremento del comercio electrónico y del homebanking generó más potenciales víctimas y atrajo a muchísimas bandas organizadas que perfeccionan a diario las estafas.

ENTENDER EL NUEVO MUNDO

- Nuestro teléfono y nuestra computadoras **ya no son nuestro teléfono y nuestra computadora**:

  Son nuestro cajero del banco, nuestra billetera, nuestra caja de seguridad, nuestro álbum privado, nuestras relaciones, nuestra exposición al mundo.

ENTENDER EL NUEVO MUNDO

- Mandarías a tus hijos de 6 años solos al cine con una mochila llena de billletes con tus ahorros?
- Irías vos con eso?
- Meterías en tu casa alguien para que te cuelgue del cable y le mostrarías un cajón lleno de billetes?

ENTENDER EL NUEVO MUNDO

- Comprarías un tv robado y le mostrarías el PIN de tu banco para que saque la plata que necesita cobrar?

ENTENDER EL NUEVO MUNDO

- EVITAR MEZCLAR PLATA Y OCIO.
- Salvo para gamers muy experimentados, no usar la computadora para jugar. Usar una consola de videojuegos.

ENTENDER EL NUEVO MUNDO

- EVITAR MEZCLAR PLATA Y OCIO.
- No instalar jueguitos en el celular.

ENTENDER EL NUEVO MUNDO

- No poner a los chicos a usar la computadora en Youtube o jueguitos online.
- Para los chicos: Usar Youtube en el TV.

ENTENDER EL NUEVO MUNDO

- NUNCA darle nuestro celular principal a los chicos.
- Usar otro teléfono viejo o una tablet SIN NUESTRAS CUENTAS.

Multiplicación de ataques automáticos

- Los dispositivos conectados a internet reciben en promedio **1.5 ataques por minuto** (celulares, computadoras, tablets, cámaras, lavarropas, etc.)

Crear ambiente digital higiénico

- Usar Windows original.
- Mantener sistema operativo actualizado (Windows, OSX, Linux, Android, iOS).
- Actualizar programas (Chrome, Office, apps de móvil, etc).

Crear ambiente digital higiénico

- No instalar apps sin fuente reconocida como empresa líder (sobre todo en Windows/Android).
- Usar siempre apps oficiales.
- Nunca instalar apps de trucos (“más seguidores de Instagram”, “funciones extras de WhatsApp”, etc.)

Crear ambiente digital higiénico

- NO USAR SITIOS WEB DE SERIES Y PELICULAS PIRATAS (usan redes grises de publicidades y pueden auto-instalar vulnerabilidades o enviar a sitios engañosos).

Si no sabés lo que es

```
curl -H "X-Header: value" https://www.keycdn.com –v
```

...no te hagas el hacker usando cosas ilegales en la web.

Crear ambiente digital higiénico: ASEGURAR NUESTRO ACCESO CRITICO

- Usar clave de acceso para la computadora y el celular.
- El PIN de 6 números es exponcialmente mejor al de 4, pero la contraseña con letras es mucho mejor.

Crear ambiente digital higiénico: ASEGURAR NUESTRO ACCESO CRITICO

- El e-mail y nuestro número de celular son los dos puntos más importantes que debemos cuidar, porque desde ahí se pueden recuperar todas las otras cuentas.

Crear ambiente digital higiénico: ASEGURAR NUESTRO ACCESO CRITICO

- NUNCA, NUNCA, NUNCA, usar la misma clave para dos sitios o redes sociales distintas.
- Si hackean un sistema, los bots buscan combinaciones repetidas de email/clave de forma automática en todas las otras redes.

COMO CREAR CLAVES SEGURAS

- La combinación ideal es Mayúsculas, minúsculas, números, signos, y al menos 11 caracteres.
- Hola!!Edd13

- Evitar usar palabras, usar acrónimos:
- Eemc (Esta es mi clave)

- **Tomar 3 caracteres del sitio/app de la clave** y mezclarlos en nuestra propia frase:
- Ejemplo con Google:
  - Hola!!gooEdd13
  - Hola!!GEddO13O (menos detectable)

- Ejemplo con Instagram:
  - Hola!!insEdd13
  - Hola!!IEddN13S

- ¿Menos reconocible? Tomar los últimos 3 caracteres o comenzar desde la segunda letra:
- Google o Google:
  - Hola!!oogEdd13 / Hola!!gleEdd13
  - Hola!!OEddO13G / Hola!!GEddL13E

- Instagram o Instagram:
  - Hola!!nstEdd13 / Hola!!ramEdd13
  - Hola!!NEddS13T / Hola!!REddA13M

- La mejor combinación: Acrónimos Eemc!!gooYnlu2v (Esta es mi clave Google!! Y no la uso 2 veces)

- Google o Google:
  - Eemcoog!!Ynlu2v / Eemc!!gle!!Ynlu2v
  - EemcO!!YnluO2vG / EemcG!!YnluL2vE

- Instagram o Instagram:
  - Eemcnst!!Ynlu2v / Eemcram!!Ynlu2v
  - EemcN!!YnluS2vT / EemcR!!YnluA2vM

- Eemco!!!oYnlug2v
- Eemcn!!!sYnlut2v
- Eemca!!!cYnlue2v
- Eemci!!!kYnlut2v
- Eemci!!!cYnlur2v
- Eemci!!!nYnluk2v
- Eemca!!!nYnlua2v
- Eemce!!!tYnluf2v
- Eemcp!!!oYnlut2v

- Eemcoog!!!Ynlu2v
- Eemcnst!!!Ynlu2v
- Eemcace!!!Ynlu2v
- Eemcikt!!!Ynlu2v
- Eemcicr!!!Ynlu2v
- Eemcink!!!Ynlu2v
- Eemcana!!!Ynlu2v
- Eemcetf!!!Ynlu2v
- Eemcpot!!!Ynlu2v

- Eemcoog!!!Ynlu2v Google
- Eemcnst!!!Ynlu2v Instagram
- Eemcace!!!Ynlu2v Facebook
- Eemcikt!!!Ynlu2v Tiktok
- Eemcicr!!!Ynlu2v Microsoft
- Eemcink!!!Ynlu2v Linkedin
- Eemcana!!!Ynlu2v La Nacion
- Eemcetf!!!Ynlu2v Netflix
- Eemcpot!!!Ynlu2v Spotify

Crear ambiente digital higiénico:
ASEGURAR NUESTRO ACCESO CRITICO

- Instalar Microsoft Authenticator o Google Authenticator y usar SIEMPRE acceso de autenticación con dos factores (2FA) para todas nuestras cuentas.

Crear ambiente digital higiénico:
ASEGURAR NUESTRO ACCESO CRITICO

- **NUNCA permitir que las notificaciones se vean con la pantalla bloqueada.**
- Si nos roban el teléfono eso les da acceso directo a nuestro Mercado Pago/PayPal, y de ahí a nuestro banco.

Crear ambiente digital higiénico:
ASEGURAR NUESTRO ACCESO CRITICO

- **No usar billeteras virtuales desde la web (Mercado Pago y similares) porque la sesión no expira.**

Crear ambiente digital higiénico:
¿Qué hacer si nos roban el teléfono?

- **Dar de baja el chip no es suficiente.**
- **Find my phone.**
- **Cuidado con las estafas de recuperación.**
- Cerrar remotamente las sesiones.

Crear ambiente digital higiénico:
ASEGURAR NUESTRO ACCESO CRITICO

- **Revisar que los sitios sean seguros HTTPS://**
- **Evitar usar redes públicas de WI-FI.**

Compras online / Billeteras virtuales:

- Nunca usar nuestra tarjeta de débito principal.
- Usar tarjeta de crédito para Mercado Pago/Paypal (se pueden negar los gastos).
- Si usamos débito para compras online, usar tarjetas temporales con saldo prepago (Lemon, Wise, etc.)

Compras online / Billeteras virtuales:

- Usar sitios de confianza y sus sistemas de seguridad incluidos (no puentearlos para evitar comisiones).
- En Facebook Marketplace solo cash (robos con comprobantes de transferencia falsos).

MercadoLibre, Booking o Marketplace:

Te envían a tu CBU dinero con 1 o 2 ceros de más.

($50.000 en vez de $5.000) y te piden reembolso por el error, pero en realidad estás gastando un crédito a tu nombre.

MercadoLibre, Booking o Marketplace:

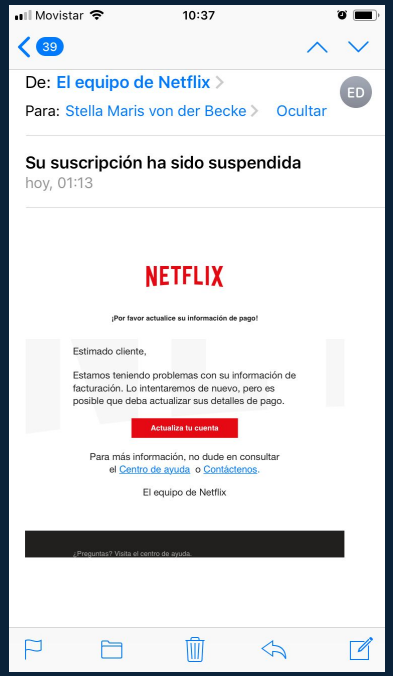
- Te piden el PIN o Token o código de recuperación enmascarado en cualquier otra cosa.
- Te piden
  - “VALIDACION DE DATOS” por otros asuntos.
  - Capturas de pantalla del mensaje.

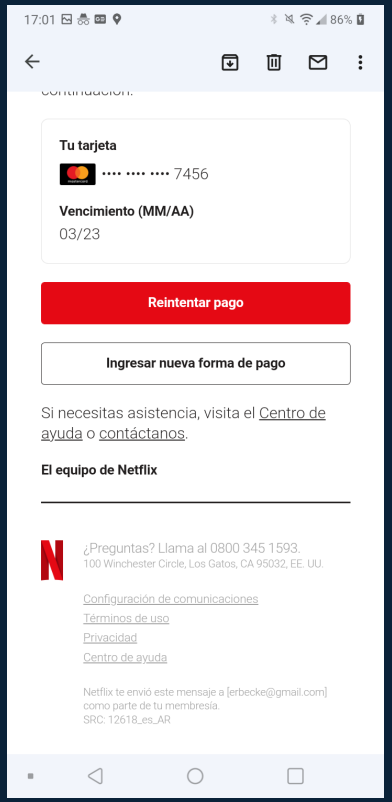
LOS ROBOS MAS COMUNES:

NUNCA, NUNCA, NUNCA “validar los datos” , ni en una pantalla, ni por llamada telefónica, ni por WhatsApp.

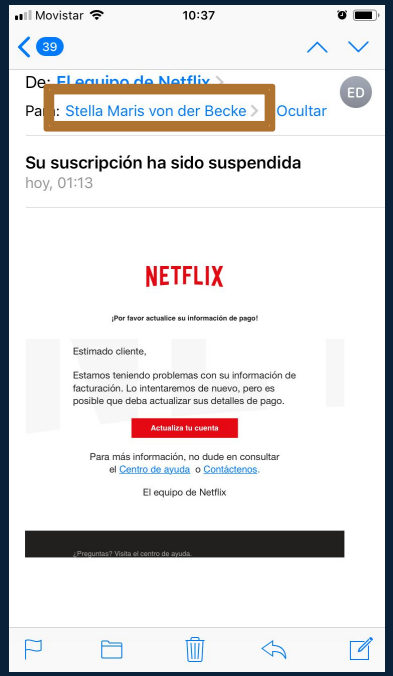
Netflix, Spotify, Personal, Reembolsos erróneos, Flybondy, Aerolíneas, obras sociales, vacunas y lo que sea... **Todo esto se usa HOY para robar tu plata.**

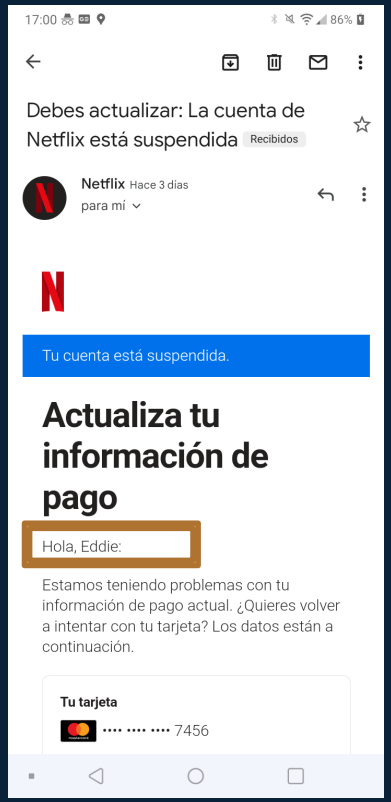
CUÁL ES EL REAL Y CUÁL ES EL FALSO??

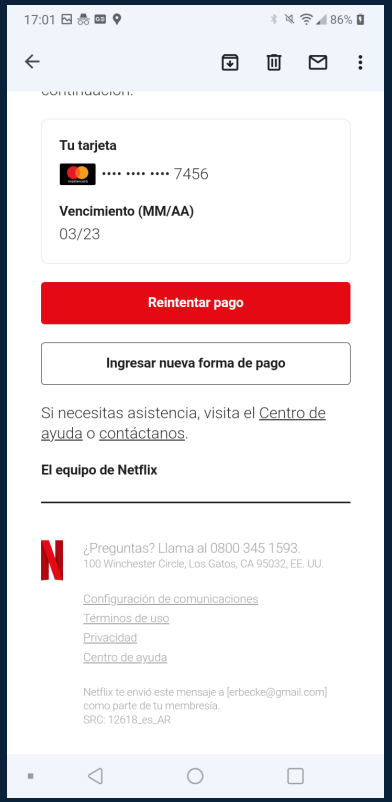




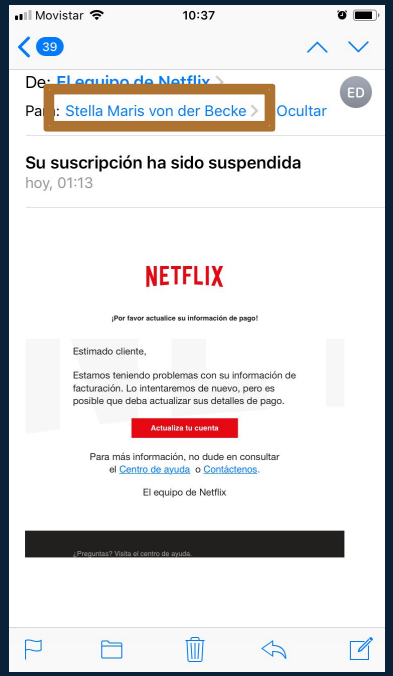
CUÁL ES EL REAL Y CUÁL ES EL FALSO??

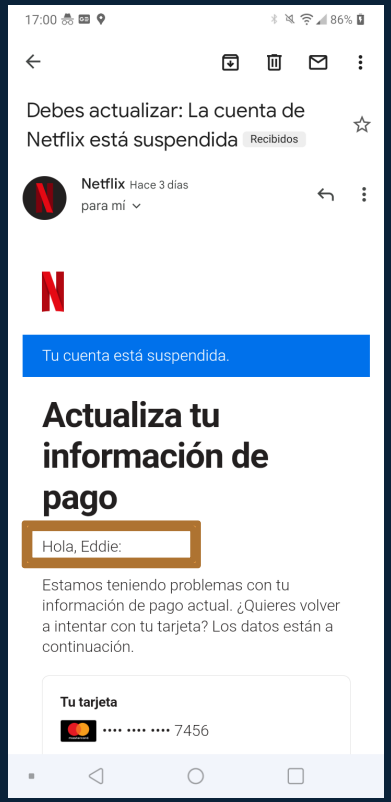






CUÁL ES EL REAL Y CUÁL ES EL FALSO??





”Su cuenta fue hackeada”

“Usted ha cometido un delito”

“Necesita validar sus datos”

“Necesita actualizar sus datos”

“Su sesión ha espirado, ingrese por aquí”

“Su clave ha sido desactivada, ingrese la actual”

“Hemos cancelado su servicio”

“Hemos descontado $xxxxxx”

“Su reembolso está listo”

NUNCA HACER CLICK DESDE EL MAIL, AUNQUE SEA EL REAL.

SIEMPRE INGRESAR DESDE LA APP O EL NAVEGADOR TIPEANDO LA DIRECCIÓN A MANO

Las estafas virtuales tienen dos características importantes:

Apelan a la **urgencia** y a la **despersonalización.**

“tu servicio se suspenderá…”

La gente no valida que sea la persona o entidad REAL.

Mensajes privados por redes sociales de nuestros contactos, pidiendo un favor de urgencia.

- *“Cambio dólares a $240 de urgencia.”*
- *“No puedo ingresar a mi usuario, te mandé un link de denuncia, pasame el código que te da para seguir el trámite.”*

- Clonan identidad de WhatsApp/Instagram y mandan mensaje con otro número:
  - *“Hola Eddie tanto tiempo! Cambié mi número!”*
  - y luego…
    - *“…ayudame con…”*

E-mails pidiéndote el número de contacto para que ELLOS TE LLAMEN (no validás la identidad) así ahorrás tiempo de espera.

Mensajes con enlaces de validación.

La lista es interminable y cambia cada semana.

Pensar quién inició el diálogo:

¿Quién envió el primer mail?
¿Quién hizo la llamada?
¿Quién contactó a quién?
¿Validé la identidad?

La lista es interminable y cambia cada semana.

Criterios importantes: Nunca compartir tus datos, aunque creas que estás hablando con la empresa.

Gracias!

¿Preguntas?

@erbecke