8.11

Phishing

¿Qué es “Phishing”?

El “Phishing” es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva.

Viene del inglés *“fishing”* que significa pescar. **Es una técnica de ciberdelincuencia que utiliza el fraude, el engaño y el timo para manipular a sus víctimas y hacer que revelen información personal confidencial.**

Veamos un ejemplo. ¿Notan algo sospechoso en el siguiente email?

Para *fede@gmail.com*

De *soporte@microsolft.com*

Urgente actualización de datos | Microsoft

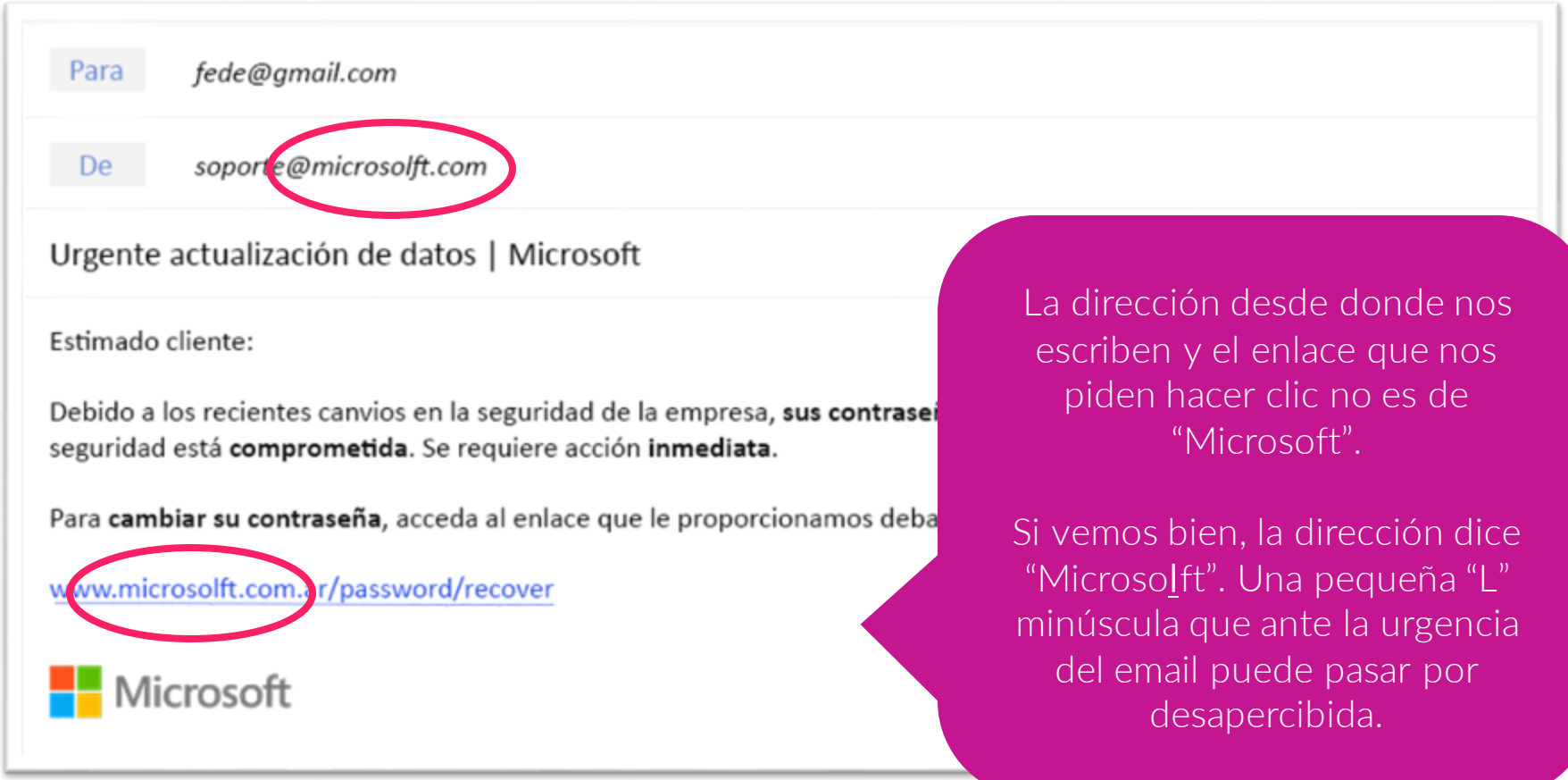
Estimado cliente:

Debido a los recientes canvios en la seguridad de la empresa, **sus contraseñas se encuentran en peligro inminente** y su seguridad está **comprometida**. Se requiere acción **inmediata**.

Para **cambiar su contraseña**, acceda al enlace que le proporcionamos debajo:

www.microsolft.com.ar/password/recover

Microsoft



La dirección desde donde nos escriben y el enlace que nos piden hacer clic no es de "Microsoft".

Si vemos bien, la dirección dice "MicrosoIft". Una pequeña "L" minúscula que ante la urgencia del email puede pasar por desapercibida.

Método “CASA” para recordar siempre que abramos un correo electrónico.

C
A
S
A

Contacto

Siempre revisa la dirección desde donde te mandaron el mensaje y comprobá que sea la correcta accediendo a la web o a mensajes anteriores de la organización/persona que te esté contactando. También es común ver errores de ortografía.

C

A

S

A

Apuro

Si te escriben cosas como “estás en peligro, resuelve ahora…”, permanecé calmado/a y analizá la situación lentamente. Es un intento de asustarte para nublar tu juicio y que tomes decisiones bajo presión.

C

A

S

A

Salida

El objetivo del “phishing “ es lograr que entres a un sitio web o descargues un archivo. Nunca dejes la seguridad de tu casilla de correo / mensaje de texto antes de estar muy seguro que confías en quien te contacta.

C
A
S
A

Ayuda

Si sospechás que fuiste víctima de “phishing ” y tus datos están en peligro, acudí lo antes posible a tus organizaciones de confianza. Hay muchos mecanismos preparados para ayudarte.

Practiquemos, ¿cuál de los siguientes correos es un ataque bajo la forma de “phishing?

De: security@paypal.com

Su cuenta fue suspendida

Su cuenta ha sido suspendida por razones de seguridad, ya que se detectó intentos de uso desde localizaciones no registradas.

Para volver a activar la cuenta le pedimos por favor que ingrese a su cuenta y siga los pasos correspondientes.

De: security@paypai.com

PayPal

Necesitamos de tu ayuda

Su cuenta ha sido suspendida, ya que se detectó un error en su información. La razón del error no es segura, pero por razones de seguridad, hemos suspendido su cuenta temporalmente.

Necesitamos que actualice su información para un uso posterior de su cuenta de PayPal.

Actualizar mi información

La 2da opción es un ataque de phishing. Veamos dónde está la evidencia.

De: security@paypai.com

PayPal

Necesitamos de tu ayuda

Su cuenta ha sido suspendida, ya que se detectó un error
información. La razón del error no es segura, pero por razo
seguridad, hemos suspendido su cuenta temporalmente.

**Necesitamos que actualice su información para un uso
de su cuenta de PayPal.**

Actualizar mi información

Primero, la dirección está mal escrita por ende es falsa. En vez de decir PayPal dice PayPai.

Segundo, debemos sospechar de que es un email urgente o que alguien necesita de nuestra ayuda.

Por último, no debemos nunca en este tipo de email hacer clic en un enlace o botón.


EidoS
ALWAYS LEARNING


INEFOP