



Potencial Digital

Cáceres, 24 y 25 de septiembre

Taller II – BEC



Taller 2: Bussines Email Compromise

TALLER 2 - BEC

LA TRANSFERENCIA DE 8.650 €

Es viernes, 16 de octubre de 2026. En administración están hasta arriba, el cierre del trimestre aprieta, tanto proveedores como clientes y nosotros mismos queremos tener todo cerrado cuanto antes e irnos de finde semana con los deberes hechos.

Carlos, un administrativo encargado de los pagos, recibe el siguiente correo...

De: facturacion@ibericasuministros.com

Asunto: Nueva cuenta bancaria - Factura 3847

Buenos días Carlos,

Por motivos administrativos hemos cambiado nuestra cuenta bancaria. Por favor, realizar el pago de la factura 3847 en la siguiente cuenta:

ESXX XXXX XXXX XXXX XXXX XXXX

Os agradecemos realicéis el pago a la mayor brevedad posible, para no incurrir en gastos adicionales.

Gracias y buen fin de semana!!

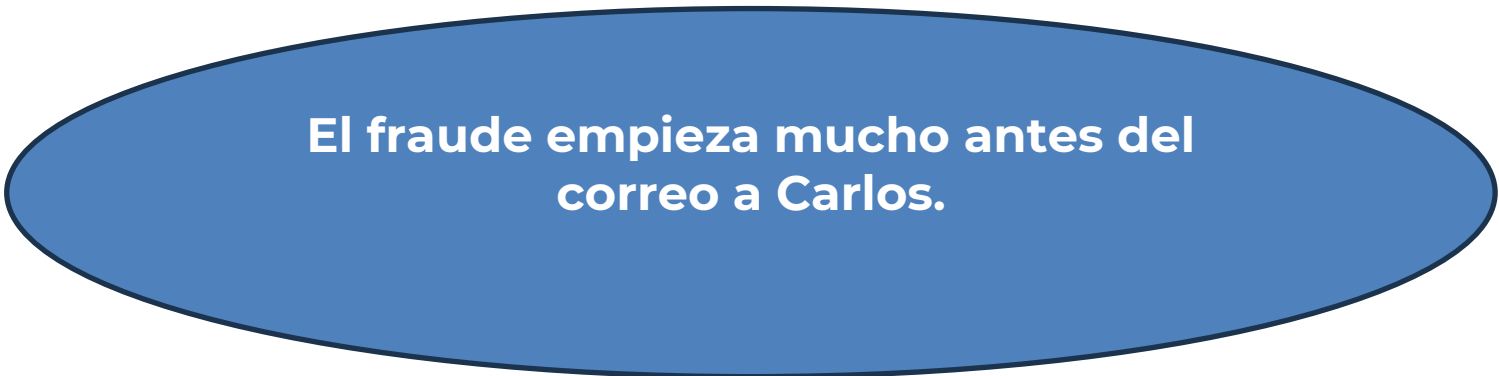
Departamento de Administración Ibérica Suministros

¿Algo que llame la atención?

TALLER 2 - BEC

LA TRANSFERENCIA DE 8.650 €

- ¿Qué ha hecho previamente el remitente del correo?
- ¿Cómo ha obtenido la información concreta sobre esa factura, su número e importe?
- ¿Y sobre el proveedor?
- ¿Y el dominio del correo, es legítimo o es “parecido”?



El fraude empieza mucho antes del correo a Carlos.

TALLER 2 - BEC

DEMO DE PHISING A CARLOS

Una semana antes, Carlos recibió el siguiente correo:

Buenos días, Carlos:

Nuestro sistema de correo electrónico ha detectado que la cuota de almacenamiento de su cuenta está próxima a alcanzar el límite establecido. Actualmente dispone de 48,7 GB utilizados de 50 GB.

Para evitar la interrupción de la recepción y envío de mensajes, es necesario validar su cuenta y ampliar temporalmente la capacidad de almacenamiento.

La validación debe realizarse antes de las 18:00 h de hoy.

[\[VALIDAR Y AMPLIAR MI CUENTA \]](#)

Si no realiza esta comprobación dentro del plazo indicado, el servicio quedará suspendido hasta completar la validación.

Gracias por su colaboración.

Soporte de correo electrónico

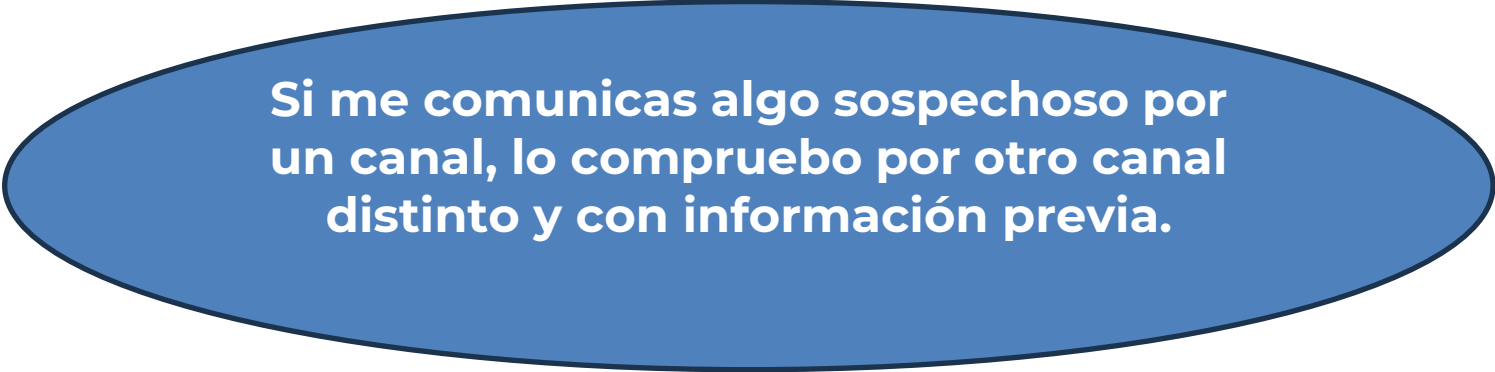
Departamento de Sistemas

¿Qué diríais que hizo Carlos?

TALLER 2 - BEC

CONCLUSIONES

- ✓ Con mecanismos sencillos (y baratos) podemos obtener una protección adecuada.
- ✓ Validar siempre las operaciones con información previa. Es decir,
 - Mail a una dirección conocida previamente.
 - Llamada a un teléfono conocido previamente, no al que venga en el correo sospechoso.
 - Preferentemente por un canal distinto, ya que si uno está comprometido se puede comprometer la validación.



Si me comunicas algo sospechoso por un canal, lo compruebo por otro canal distinto y con información previa.

BEC, Bussiness Email Compromise

¿QUÉ ES UN ATAQUE BEC?

Fraude basado en la suplantación de correos electrónicos corporativos para inducir a empleados o directivos a realizar pagos o compartir información sensible.

Las organizaciones más afectadas suelen ser las **Pymes** con procedimientos financieros poco formalizados.

1 correo puede ser suficiente para provocar una transferencia fraudulenta.

El FBI atribuye al BEC pérdidas superiores a 50.000 millones de dólares acumulados desde 2013.



Empresa de 15 empleados

Facturación anual: 1,2 M€

Correo aparentemente enviado por el gerente.

Solicitud urgente de pago a proveedor.

Transferencia realizada: 28.500 €.

El fraude se detecta dos días después.

TALLER 2 - BEC

PREGUNTAS

¿DUDAS, PREGUNTAS COMENTARIOS?

**MUCHAS GRACIAS POR TU
PARTICIPACIÓN, Y RECUERDA QUE
PODEMOS HACER MUCHO POR LA
CIBERSEGURIDAD CON SÓLO NO
ACTUAR DE FORMA IMPROVISADA!!!!!!**

Datos de contacto



Alfredo Vizcaino: <https://www.linkedin.com/in/alfredovizcaino/>

Nacho Barnés: <https://www.linkedin.com/in/nachobarnescibersecurity/>