jueves 5 de noviembre de 2026

Claves para detectar fraudes digitales y proteger tu negocio



Descargar imagen

HuelvaLAB aborda consejos prácticos para reconocer intentos de suplantación, verificar solicitudes de pago y actuar ante una estafa en una Píldora Formativa Online con Nacho Bellosta

Un mensaje que anuncia el bloqueo de una cuenta. Una llamada que parece proceder del banco. Una factura de un proveedor habitual con un número de cuenta diferente. Los fraudes digitales se introducen en gestiones cotidianas y recurren a la confianza y a la urgencia para provocar una respuesta precipitada.

Reconocer estas situaciones y adoptar hábitos de prevención centró la Píldora Formativa Online «Fraudes digitales: aprende a detectarlos para proteger tu negocio», organizada por HuelvaLAB, iniciativa de la Diputación de Huelva coordinada por el Servicio de Tecnología de la Información.

La sesión estuvo a cargo de Nacho Bellosta Sanagustín, profesional de la formación y la consultoría especializado en ciberseguridad y transformación digital. La presentación abordó situaciones que pueden afectar tanto a personas autónomas como a empresas con equipos que gestionan correos, facturas y pagos.

Una recomendación articuló el contenido de la microformación: **parar, verificar por otro canal y decidir**. Antes de facilitar información o realizar una operación conviene comprobar la solicitud a través de un contacto conocido.

Una identidad que parece real

2019 © Diputación Provincial de Huelva

El número que aparece en la pantalla del teléfono no garantiza la identidad de quien llama. La suplantación del identificador de llamadas puede hacer que una comunicación fraudulenta parezca proceder de una entidad conocida. La presentación también advirtió del uso de inteligencia artificial para imitar voces.

Algo similar ocurre con los SMS. Un mensaje falso puede aparecer en el mismo hilo que otros mensajes auténticos del banco porque el teléfono los agrupa por el nombre del remitente.

Ante una comunicación sospechosa, la pauta es interrumpir el contacto y realizar la comprobación por cuenta propia. Por ejemplo, abrir la aplicación del banco o llamar al número oficial que figura en la tarjeta. El teléfono o el enlace que facilita quien contacta no deben ser la vía de verificación.

Enlaces y facturas bajo revisión

La píldora también explicó que una web con conexión HTTPS puede ser fraudulenta. El cifrado de la conexión no acredita la legitimidad de la página. Ante un enlace dudoso resulta más seguro acceder a la aplicación habitual o escribir una dirección conocida.

En la gestión empresarial merece especial atención el fraude del proveedor. Una factura puede conservar el logotipo, los datos y el aspecto de un documento auténtico e incorporar una cuenta bancaria controlada por quienes cometen la estafa.

Por eso, **cualquier cambio de cuenta debe comprobarse mediante una llamada al contacto habitual**, con el número que la empresa ya tenga registrado. La revisión por dos personas de los pagos a cuentas nuevas o de importes elevados añade una comprobación antes de autorizar la operación.

Hábitos que refuerzan la prevención

Activar la verificación en dos pasos en el correo y en los servicios bancarios, configurar avisos de movimientos y ajustar los límites de las transferencias fueron otras de las medidas recogidas en la presentación.

Para las empresas con personal se planteó establecer un procedimiento de pagos por escrito y definir quién puede autorizar operaciones. Las peticiones urgentes, incluso cuando parecen proceder de una persona con responsabilidad en la organización, deben seguir esas mismas comprobaciones.

La formación breve y periódica del equipo y un canal claro para comunicar dudas completan estas medidas. Detectar y avisar a tiempo requiere que cualquier persona pueda informar de una sospecha sin miedo a recibir una reprimenda.

Si ya se ha realizado un pago fraudulento, la recomendación es contactar cuanto antes con el banco para solicitar que intente recuperar los fondos, conservar las pruebas y denunciar ante la Policía Nacional o la Guardia Civil. También conviene revisar las cuentas afectadas y avisar a las personas o empresas implicadas.

La sesión recordó además el **017, la Línea de Ayuda en Ciberseguridad de INCIBE**, como recurso de orientación para empresas y particulares, incluso cuando todavía no se ha producido una pérdida económica.

Con esta Píldora Formativa Online HuelvaLAB acerca pautas de ciberseguridad aplicables al trabajo diario y refuerza la capacitación digital de empresas, profesionales y proyectos emprendedores de la provincia.

2019 © Diputación Provincial de Huelva