¿Qué es el phishing y cuál es su objetivo?

El phishing es un intento de suplantación de identidad: los ciberdelincuentes se hacen pasar por una empresa, institución o servicio conocido y con buena reputación para engañarte y **conseguir robarte tus datos privados, credenciales de acceso o datos bancarios**. Esta práctica fraudulenta se apoya en la ingeniería social y está muy extendida. En ocasiones el phishing también se usa para infectar los dispositivos con algún tipo de malware (programa malicioso).

¿Cómo puede llegar hasta nosotros un caso de phishing?

La mayoría de casos de phishing se distribuyen a través del correo electrónico ya que los ciberdelincuentes cuentan con un gran número de direcciones de email que han recopilado de muy diversas formas. Por tanto, les resulta relativamente sencillo utilizar este medio para difundir sus ataques de phishing

Cómo identificar un correo electrónico fraudulento

Los ataques de phishing son eficientes porque evolucionan y se vuelven cada vez más sofisticados. A veces es difícil distinguir a primera vista un correo electrónico falso de uno original, por eso es importante que tengas en cuenta estas 5 sencillas medidas de protección:

1. Información personalizada con tu nombre
Los correos electrónicos no van personalizados en la cabecera. Un ciberdelincuente puede tener tu dirección de correo electrónico pero no tu nombre y apellidos, por lo que si la comunicación no va personalizada desconfía.

2. Datos y claves personales
Si te piden por correo electrónico o por SMS que facilites tus claves de acceso, tus datos personales o los datos de tarjetas desconfía y nunca facilites estos datos.

3. Nunca abras archivos adjuntos
En las comunicaciones por e-mail suelen enviar ficheros adjuntos, por lo que si recibes un correo de direcciones no conocidas no abras estos ficheros, podrían esconder un virus.

4. Dirección del remitente
Si la dirección del remitente del correo electrónico se presenta de forma inusual, desconfía. En ocasiones los ciberdelincuentes son capaces de falsear la apariencia del remitente, por lo que no lo tengas en cuenta como único criterio para confiar en una comunicación.

Plaza de Cervantes, 12 – 28801 ALCALÁ DE HENARES. Telf: 91 888 33 00. Ext: 1102 / 1431. E-mail: innovacion@ayto-alcaladehenares.es

5. Cuidado con dónde te llevan los enlaces
Como norma general, desconfía de cualquier e-mail que incluya un enlace a una página con un formulario donde te solicitan datos personales (número completo de la tarjeta, nombre y apellidos, DNI y clave de acceso…). Siempre es preferible que escribas tú la url de la página a la que quieres dirigirte en el navegador.

Qué debes hacer si crees que has recibido un correo electrónico fraudulento:

1. No accedas a las peticiones de solicitud de información.
2. No contestes en ningún caso a los correos.
3. No abras los ficheros adjuntos.
4. Elimina el correo y pasa el antivirus.

En caso de duda con algún correo recibido, reenvía el mismo a la dirección

it.sistemas@ayto-alcaladehenares.es

Desde el Departamento de Sistemas verificaremos el correo y te responderemos lo antes posible.

¿Cómo identificar un caso de phishing?

Generalmente los correos de phishing tienen algunas características comunes. Aquí te contamos cuáles son las pistas que deberían hacerte sospechar:

1. ***No conoces el remitente y/o el dominio no coincide con la empresa o servicio que dice ser***

   Por ejemplo, si recibes un correo en nombre del Ayuntamiento de Alcalá de Henares, y el domino del email no incluye ayto-alcaladehenares.es, es sospechoso. De la misma forma que también lo es si el correo que te llega está utilizando un servicio de correo gratuito como Gmail, Outlook, Yahoo!, etc.

2. ***El asunto es muy llamativo y/o solicita realizar alguna acción de manera urgente***

   Algunos ejemplos que pueden ayudarte: “Tiene un mensaje nuevo de seguridad”, “Detectados movimientos sospechosos”, “Eliminación de cuentas inactivas”, “Ha recibido una notificación”, “Tienes un paquete esperando”, etc.

3. ***Si la redacción del mensaje no es correcta***

   Frases mal construidas o sin sentido, palabras con símbolos o caracteres extraños, faltas de ortografía, etc. Todo esto son evidencias de que algo no va bien. Un servicio con

Plaza de Cervantes, 12 – 28801 ALCALÁ DE HENARES. Telf: 91 888 33 00. Ext: 1102 / 1431. E-mail: innovacion@ayto-alcaladehenares.es

buena reputación no te suele enviar un correo con tales síntomas. Se asegurará de que tanto la estructura y diseño del correo como su contenido sea correcto, ya que la imagen que se trasmite a los usuarios es un aspecto muy importante para cualquier servicio que se precie. Pero ojo, que también los ciberdelincuentes van mejorando sus prácticas, así que si te encuentras un mensaje sospechoso con una perfecta redacción, asegúrate de haber verificado el resto de pistas antes de darlo por bueno.

4. ***El mensaje está poco o nada personalizado***

   Comunicaciones anónimas del tipo "Estimado cliente", "Notificación a usuario" o "Querido amigo", son indicios que te deben poner alerta. Si un delincuente quiere estafar a cientos de miles de personas, es muy complicado que pueda saber el nombre de todas ellas. Por eso utilizan fórmulas genéricas como las mencionadas.

5. ***Te obligan a tomar una decisión en unas pocas horas***

   Con amenazas de que en caso contrario tendrás algún problema: bloqueo de cuenta, problemas de seguridad, una multa o sanción, etc. Frases como "Si el registro no es realizado dentro de 48 Horas su cuenta será suspendida temporalmente hasta que su registro sea completado", "Hemos detectado que no ha finalizado correctamente su sesión, por favor, pinche aquí para hacerlo", "Por mejoras en nuestras políticas de seguridad, por favor, haga clic aquí para cambiar sus claves", "Ha recibido una notificación pero no se encontraba en casa, descargue el código adjunto para poder ir a recogerlo" son pistas que te pueden ayudar a identificar posibles fraudes.

6. ***El texto del link facilitado en el correo no coincida con la dirección URL a la que apunta***

   La intención de los delincuentes es que pinches en un enlace para llevarte a un sitio web fraudulento en lugar de a la página legítima. Por tanto, es importante comprobar que el enlace es fiable. Para ello, puedes situar el puntero del ratón encima del enlace y observar la dirección que se muestra en la parte inferior izquierda del navegador o de tu cliente de correo. Si lo que ves es sospechoso, ¡no hagas clic! Como norma general, además, nunca te enviaremos un correo electrónico con un enlace a una web donde te solicita datos personales, de tus cuentas o tarjetas.

7. ***Un documento adjunto tiene más de una extensión o viene en un .zip o .exe.***

   Si a las pistas anteriores le sumamos que el mensaje que recibes te invita a descargar un fichero que, curiosamente, tiene más de una extensión, algo en esta línea "nombredelfichero.doc.zip" o se trata de un fichero comprimido (.zip) o un ejecutable (.exe), no se te ocurra descargarlo o es más que probable que tus dispositivos acaben infectados. En cualquier caso, si confías en la fuente y optas por la descarga del fichero, analízalo siempre con un antivirus antes de abrirlo y ejecutarlo.

Plaza de Cervantes, 12 – 28801 ALCALÁ DE HENARES. Telf: 91 888 33 00. Ext: 1102 / 1431. E-mail: innovacion@ayto-alcaladehenares.es