Estafas informáticas relacionadas con la vacunación

Mientras todos esperamos el fin de la pandemia de coronavirus, muchas personas están comprensiblemente centradas en la vacuna COVID-19. **Hoy en este breve artículo, yo José Luis Martir Millán, junto con mi equipo de peritos, te explicaremos todo sobre las estafas informáticas de la actualidad y cómo un perito informático forense puede ayudarte.**

Hoy en día, todos quieren vacunarse. Los estafadores lo saben. Y mientras tú sueñas con abrazar a tus seres queridos, ir a conciertos, o simplemente sentirte seguro dentro de una tienda, ellos están ocupados elaborando campañas de phishing relacionadas con la vacuna para engañarte y hacerte entregar información personal, dinero o acceso a tu dispositivo.

¿Sabes qué es el Smishing?

Cómo se muestran las estafas relacionadas con las vacunas según un perito informático forense

Los estafadores en línea han utilizado durante años las crisis y los grandes acontecimientos para estafar a la gente. La pandemia ha creado una situación atractiva porque todo el mundo es consciente de la enfermedad y de las dificultades que ha causado en la vida de todos.

Desde el punto de vista de los delincuentes, es una gran oportunidad para conseguir que mucha gente actúe en contra de su buen juicio. Los estafadores aprovecharon esta oportunidad tan pronto

como la pandemia se afianzó, ofreciendo curas de aceite de serpiente que nunca se materializaron a cambio de números de tarjetas de crédito o de hackear los ordenadores de sus objetivos.

Ahora las vacunas ofrecen a los estafadores otro señuelo para sus objetivos. Las estafas, pueden ser "increíblemente convincentes", sobre todo para las personas mayores, que encabezan las listas para vacunarse y pueden estar esperando noticias de las autoridades médicas.

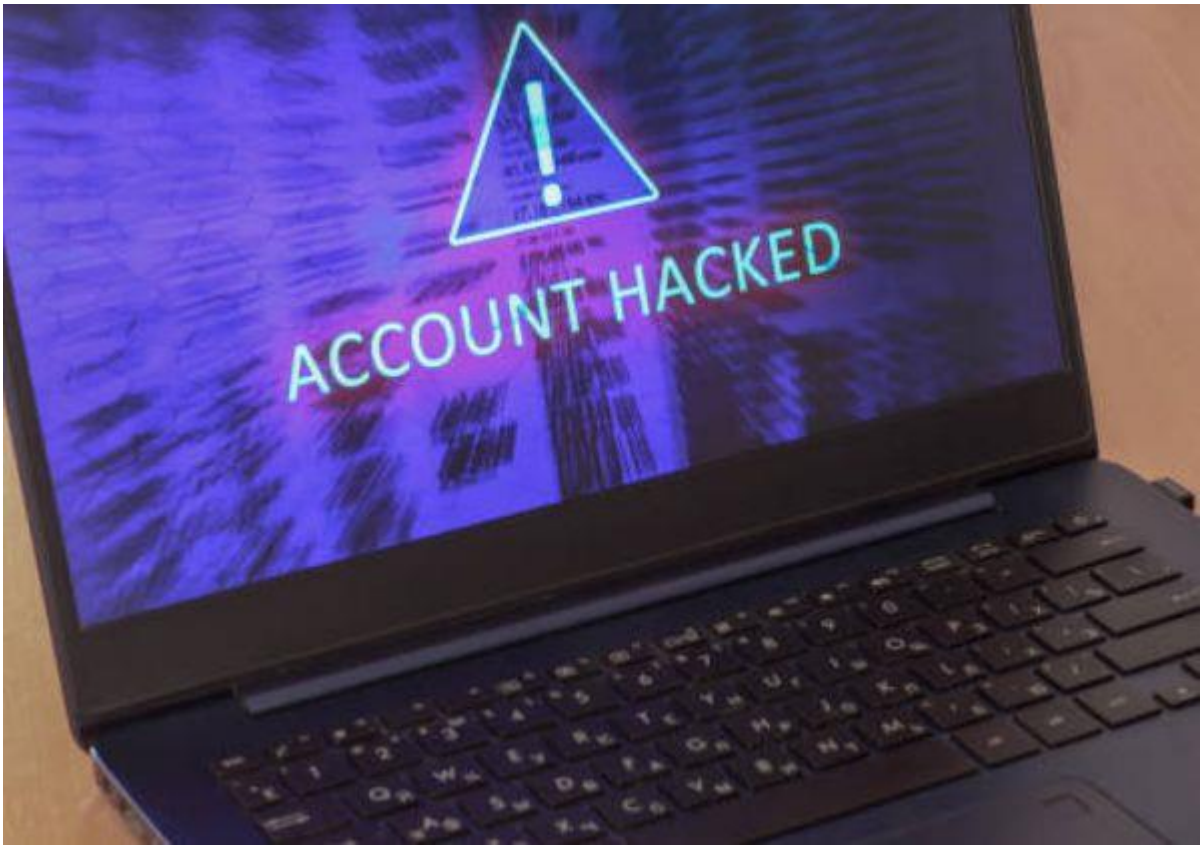
Los estafadores están comprando anuncios que ofrecen la venta de vacunas directamente a los usuarios de Internet. Es probable que solo quieran robar la información de tu tarjeta de crédito, pero incluso si enviaran algo que pretendiera ser una vacuna, sería extremadamente peligroso. Conoce algunas estafas frecuentes:

Estafas bien preparadas

Los estafadores suelen registrar un nuevo nombre de dominio relacionado con su estafa cuando preparan una campaña de phishing, para que sirva de reclamo a sus objetivos. Los sitios web pueden contener formularios de apariencia legítima destinados a robar información de pago o de atención sanitaria, o pueden alojar software malicioso que se instala en su dispositivo cuando lo visita.

El software malicioso, o malware, puede dejarle vulnerable a ataques de ransomware, anuncios emergentes que inutilizan su dispositivo y otros ataques intrusivos de los hackers.**Por lo general, te encontrarás con una estafa de vacunas mediante un mensaje convincente diseñado para que respondas.**

El peritaje informático ha encontrado correos electrónicos con líneas de asunto que incluyen temas relacionados con las vacunas. **Estos mensajes contenían un archivo malicioso que habría infectado los ordenadores de los destinatarios con malware si se abría.**



Aprende [cómo saber si alguien ha entrado en nuestro Gmail]

Anuncios fraudulentos de vacunas

Si buscas en Internet información sobre vacunas, es posible que más adelante veas anuncios en varios sitios web sobre dosis de vacunas que puedes pedir por Internet.

Los estafadores compran estos anuncios porque saben que tú estás interesado en las vacunas, al igual que los minoristas legítimos pueden mostrarte anuncios de botas de lluvia durante días después de que busques ropa para el clima húmedo.

Los anuncios de vacunas son otra estafa destinada a recopilar tu información financiera. Los investigadores de empresas de detección de fraudes han encontrado en la web venta de vacunas, pero el negocio es claramente fraudulento.

Incluso si la empresa enviaba algo que decía ser una vacuna, la venta directa de la verdadera vacuna COVID-19 es casi imposible debido a lo costoso que es mantener el rango de temperatura de frío adecuado para el paquete en todo momento.

Cómo evitar el fraude relacionado con las vacunas

En general, se hace un llamado a la gente a desconfiar de cualquier correo electrónico, mensaje de texto o llamada telefónica que provenga de un remitente no reconocido y que ofrezca información sobre la vacuna contra el coronavirus.

Al igual que con cualquier mensaje de un remitente desconocido, no hagas clic, no descargues ni compartas tus contraseñas. Obtén la información sobre las vacunas de fuentes oficiales, como los departamentos de salud estatales y locales, la Administración de Alimentos y Medicamentos y su médico.

Descubre qué es y de qué se trata el servicio de Laboratorio Informática Forense

Además, ten en cuenta que tu información sanitaria también puede ser utilizada para el robo de identidades médicas. Facilita tu seguro o información sanitaria solo a profesionales que conozcas y en los que confíes, y controla tus reclamaciones al seguro para asegurarte de que nadie más está utilizando su seguro médico.

Consejos para evitar ser parte de una estafa informática relacionada con las vacunas

Lamentablemente los estafadores informáticos no descansan, todo lo contrario. **En las crisis como la que estamos viviendo en este 2021 es cuando más aprovechan la oportunidad de dañar a otros.**

Debes estar muy atento a tu actividad en línea, sigue estos consejos dados para evitar encontrarte en esta desagradable situación:

- No pagues para que te coloquen la vacuna. Cualquier persona que te solicite un pago para colocarte en una lista, darte una cita o un cupo es evidentemente una estafa.
- Ignora los anuncios de venta de la vacuna COVID-19. No puedes comprarla en ningún sitio, incluidas las farmacias online. La vacuna solo la encontrarás disponible en instituciones aprobadas por el gobierno, por ejemplo en farmacias y centros de vacunación.
- Está atento a los textos inesperados o inusuales. No entres a los enlaces de los mensajes, especialmente a los que no estás esperando. Si tus proveedores médicos o farmacéuticos anteriormente se han comunicado contigo por mensajería de texto, es posible que recibas un mensaje sobre la vacuna.
- Si recibes un mensaje de texto, llama directamente a tus proveedores de atención médica o farmacéutico para asegurarte de que te lo han enviado. Los estafadores también envían textos y se hacen pasar por otras personas.
- No abras correos electrónicos, archivos adjuntos o enlaces de personas que no conozcas o que lleguen de forma inesperada. Podrías descargar peligrosos programas maliciosos en tu ordenador o teléfono.
- No compartas tu información personal, financiera o de salud con personas que no conoces. Debes saber que ningún personal que distribuya vacunas, de consultorios médicos, de farmacias o de una compañía de seguros médicos se contactará contigo.
- Recuerda que nadie te llamará, enviará un mensaje de texto o un correo electrónico para pedirte datos de tu seguro, de tarjeta de crédito o de cuenta bancaria para inscribirte en la vacunación.

Conoce [10 Consejos prácticos para mejorar la seguridad informática]

En resumen, no puedes pagar para evitar las filas, reservar un cupo o apuntarte a un ensayo crítico**. Desconfía de cualquier llamada o mensaje de texto que te pida datos personales como datos financieros o información del seguro para reservar tu cupo.**

Con la tecnología avanzando el riesgo informático siempre está presente, te recomendamos que cuides muy bien tu información personal y tomes las respectivas medidas de seguridad en tus sistemas y redes sociales que usas día a día.

Esperamos que con estos consejos no llegues a ser víctima de las estafas informáticas relacionadas con la vacunación, pero si esto llegara pasar y necesitas ayuda profesional no dudes en contactar un perito informático forense en peritinformatic.com y con gusto te ayudaremos a resolver tu situación. **Contáctanos ya al siguiente correo electrónico lluis@peritinformatic.com.**