| Logo instituto sin fondo |
| --- |
| **INSTITUTO SUPERIOR DE FORMACIÓN TÉCNICA N° 93****CARRERA:** Tecnicatura superior en análisis, desarrollo y programación de aplicaciones**ESPACIO CURRICULAR:** Metodología de Investigación**CURSO:** 1 AÑO B**CICLO LECTIVO:** 2024**PROFESORA:** Sciacca Carolina**ALUMNO:** Nicolás Sandoval**ALUMNO:** Demchum Lautaro**CANTIDAD DE HOJAS:** |

La Ciberseguridad y las personas mayores

### Cómo interactúan las personas mayores en las redes sociales y cómo las afectan estas en la vida real

#### Introducción

Las redes sociales, han comenzado a generar un gran impacto alrededor del mundo, esto sucedió a partir de los últimos años de la década de 1990, ganando exponencialmente una gran cantidad de suscriptores a través de aplicaciones web. Como consecuencia, algunos usuarios vieron que podían introducir sus intenciones maliciosas para lograr un objetivo muy claro, el cual sería el aprovechamiento de la ignorancia que tienen las personas hacia algo nuevo y masivo que estaba llegando, que hasta el día hoy es muy difícil poder contrarrestar.

Estas intenciones maliciosas son mejor conocidas como Ciberataques Informáticos, que pueden ser de muchas formas posibles, entre ellas está el robo de datos personales o empresariales, como los números de identidad y las claves bancarias, las estafas a personas adultas con bajos conocimientos en el manejo de internet, a través de distintos medios informáticos que podrían llegar a ocasionar múltiples problemas a los equipos que estamos manipulando o la persona misma.

A partir de lo antes expuesto, es de donde vamos a plantear nuestro objetivo, este será identificar las formas de contrarrestar, prevenir y repeler los ciberataques a los adultos mayores vulnerables que son atrapadas en las redes sociales que tanto entretenimiento tienen para dar. Pero para poder realizarlo se tiene que saber que es la ciberseguridad y las maneras que tiene para poder lograrlo.

Estas cuestiones serán desarrolladas y nos servirán de hilo conductor durante todo el estudio de investigación para comprender ante lo que nos enfrentamos, intentando alcanzar la problemática que planteamos.

Entonces ¿Qué es la ciberseguridad? ¿Qué tan importante es? ¿Cómo ayuda a contrarrestar los ataques? ¿Cuáles son sus métodos de prevención? ¿Puede repeler estos ataques de alguna manera?.

#### ¿Qué es la ciberseguridad?

Es el método desarrollado por las personas científicas especializadas en la informática para combatir las malas intenciones de usuarios ajenos a los primeros sistemas que se establecieron.

Estos surgieron hace ya más de 50 años, cuando se empezaron a conectar las computadoras mediante una red y módems. Esto quiere decir que antes solo se podía piratear una computadora únicamente de manera física, frente al monitor de la misma. Pero ese delito aún no se lo consideraba como un ciberataque, solo se lo caratulaba como violación de la privacidad. Así fue como en la década de 1960 comenzó lo que hoy conocemos con esta forma de red.

La ciberseguridad intenta proteger equipos, redes, aplicaciones, sistemas de alta complejidad y principalmente los datos de personas ante las amenazas digitales que muchos escucharon pero que pocas saben cómo enfrentar.

Las organizaciones utilizan medidas y herramientas para proteger los datos confidenciales, como también los accesos no autorizados, para evitar interrupciones en los sistemas bancarios u otros sistemas de alta complejidad como lo es el transporte. La ciberseguridad implementa la defensa en las organizaciones mundiales mediante leyes y estatutos como los hay en Europa, que deben cumplir el Reglamento General de Protección de Datos (GDPR). ¿Cuál es el objetivo de este reglamento? proteger a las personas cuando sus datos están siendo tratados por el sector privado y la mayor parte del sector público y también permite que las personas controlen mejor sus datos personales

Además de lo antes dicho, está la ciberseguridad en el tema que queremos abordar, que es la que se encuentra en las redes sociales. Las medidas tomadas acá son muchas e incluyen el uso de contraseñas fuertes, que contienen letras minúsculas, mayúsculas, números y caracteres especiales, la autenticación en dos pasos, que consiste en el envío de código a teléfonos para confirmar antes de un tiempo determinado, o también un dispositivo con sistemas biométricos y reconocimiento facial.

Además estas aplicaciones sociales ofrecen vigilancia constante de las actividades en la cuenta y notificación de posibles incidentes, la implementación de políticas de seguridad para los empleados y usuarios, y por último, el monitoreo y respuesta rápida a posibles incidentes de seguridad.

Como podemos observar, cuando comenzó el auge de las redes sociales, todas estas implementaciones, aún no estaban impuestas, solo se necesitaba un correo electrónico, un pequeño formulario y una contraseña sin estándares para poder suscribirse a una página web de chat online. Comenzar a ser un usuario más de estas redes no era tarea difícil, cualquier persona con acceso a internet podía hacerlos en menos de dos minutos.

Es por esta razón que se empezaron a esparcir de manera exponencial los diferentes tipos de ataques informáticos que conocemos, entre los más conocidos están Malware, Ransomware, Ataque de intermediario, Phishing, DDoS, Amenaza interna, todos ellos hacen una gran navaja suiza que ayuda los muchos dolores de cabeza y cantidades de trabajo que terminan realizando los administradores de seguridad informática de las empresas.

Como pueden apreciar, algunos de estos ataques al ser de una reciente innovación técnica que se están implantando en la cultura social que estamos, tienen palabras que son neologismos, ya que su composición está relacionada a partir de dos palabras ya existentes, como por ejemplo Malware, que está formada por dos palabras. Una de ellas es la palabra malicious, que viene del inglés, esta significa malicioso, y de palabra màs, que es Software, que también es otro neologismo, que su estructura proviene de la palabra inglesa soft que significa suave, y ware que proviene del inglés que significa componente. Es por eso que Malware significa componente malicioso.

Pasemos a explicar, de qué se trata cada ataque informático, para entender su funcionamiento y la finalidad de su creación. Solo así vamos a poder comprender cómo los administradores de la seguridad cibernética analizan y desarrollan su trabajo, y depende de la empresa en la que se encuentren, lo harán durante el día y la noche. Empecemos con la que más porcentaje de daños ha causado, esta es el Malware.

#### Malware

Como habíamos dicho anteriormente, Malware significa software malicioso, este lo puede ser de muchas maneras, las principales son dañar una computadora, infiltrarse y apoderarse del control absoluto del sistema informático sin los permisos de los administradores, entre los que se encuentran:

1. **Virus**: Programas que se adjuntan a otros archivos y se propagan cuando esos archivos se comparten tal cual como pasa en la vida real.
   * **Ejemplo**: **ILOVEYOU** - Un virus que se propagó a través de correos electrónicos en el año 2000, causando daños masivos.
2. **Gusanos**: Similar a los virus, pero no necesitan adjuntarse a otros archivos para propagarse.
   * **Ejemplo**: **Wanna Cry** - Un gusano que afectó a miles de computadoras en 2017, con un cifrado de archivos y pidiendo un rescate.
3. **Troyanos**: Programas que se disfrazan de software legítimo para engañar a los usuarios y obtener acceso a sus sistemas.
   * **Ejemplo**: **Zeus** - Un troyano que roba información bancaria y credenciales de acceso.
4. **Spyware**: Software que recopila información sobre el usuario sin su conocimiento.
   * **Ejemplo**: **Keylogger** - Un tipo de spyware que registra las pulsaciones del teclado para robar contraseñas y otra información sensible.
5. **Adware**: Software que muestra anuncios no deseados y a veces maliciosos.
   * **Ejemplo**: **Fireball** - Un adware que secuestran navegadores y muestra anuncios intrusivos.
6. **Ransomware**: Malware que cifra los archivos del usuario y exige un pago para desbloquearlos.
   * **Ejemplo**: **CryptoLocker** - Un ransomware que cifra archivos de usuarios y pide un rescate en bitcoins.

Estos son algunos de los ejemplos de tipos de Malware que existen, pasemos a ver uno de los que siguen, y seguir informandonos sobre los ataques informáticos. El siguiente se trata de uno de los antes vistos y es de los que más aparecen durante nuestro recorrido por el internet.

#### Phishing

La expresión phishing es utilizada para definir a un tipo de fraude que tiene por objetivo engañar a la persona usuaria para que revele algún tipo de información, generalmente financiera o personal, con el objetivo de suplantar su identidad digital y obtener algún beneficio. Se trata del ciberataque más común y más sencillo, y quien lo perpetra suele ser denominado “phisher”.

El phishing que utiliza señuelos de correo electrónico se ve obstaculizado por tecnologías de filtrado avanzadas y requisitos de envío, lo que hace que sea más difícil para los estafadores hacer llegar sus correos electrónicos a las bandejas de entrada de las víctimas, en ese contexto aparece el vishing (en el que los estafadores llaman a las víctimas potenciales) y el smishing (en el que los estafadores publicitan las URL de sitios de phishing en SMS y mensajes de texto) y en el phishing híbrido, el estafador envía un correo electrónico o un mensaje de texto que solicita al destinatario que llame a un número de teléfono. Esto le permite al estafador hablar directamente con las víctimas potenciales y manipularlas de primera mano.

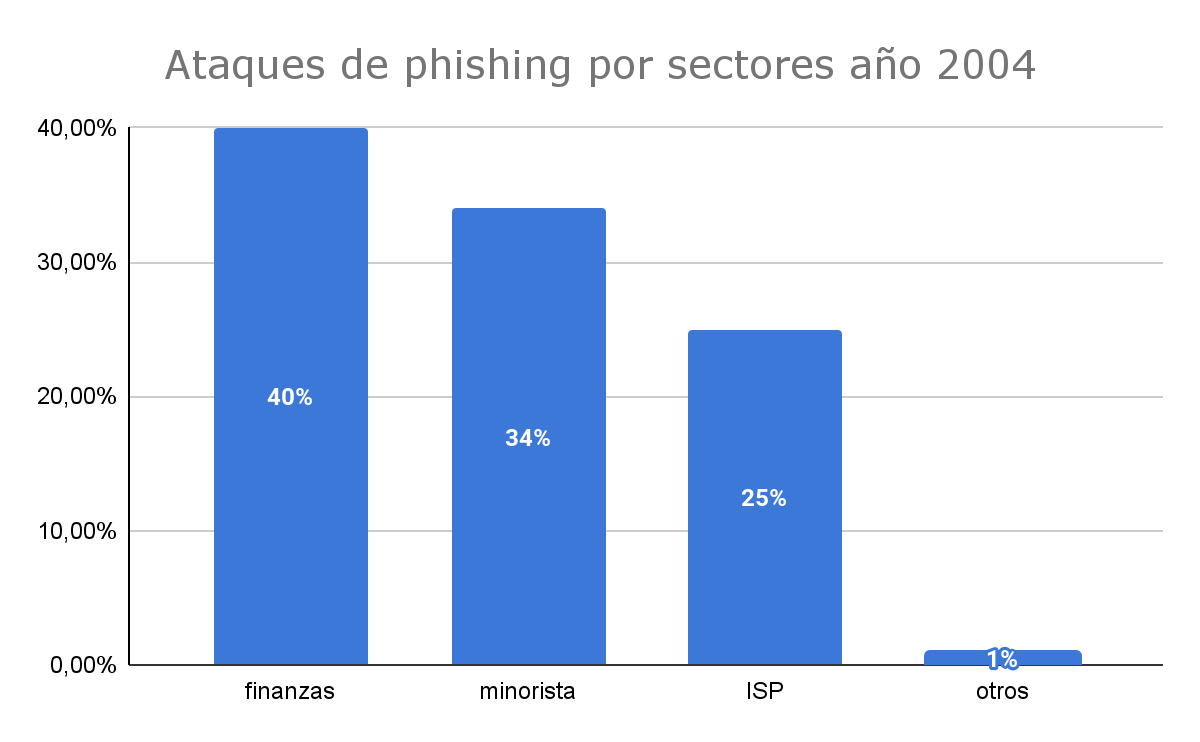
### Recomendaciones para evitar el Phishing

Vamos a plantear algunas formas de evitar estos ataques, en especial los de phishing, que al ser tan simple podemos toparnos con él en cualquier momento, cuando más bajes la guardia, en ese momento es cuando los phishers van a estar atentos.

Una de estas formas son bastante tediosas, ya que estamos acostumbrados a que las aplicaciones las hagan por nosotros, como lo son las cuentas bancarias, estas llevan una completa lista de los movimientos que hacemos, entonces ¿cuál es la recomendación? es simple, solo verificar por nuestra cuenta los movimientos que hacemos, en muchos casos los bancos no se alertan de un movimiento extraño que no solemos hacer, es por eso que debemos fijarnos y asegurarnos de que no fuimos ataques de manera silenciosa.

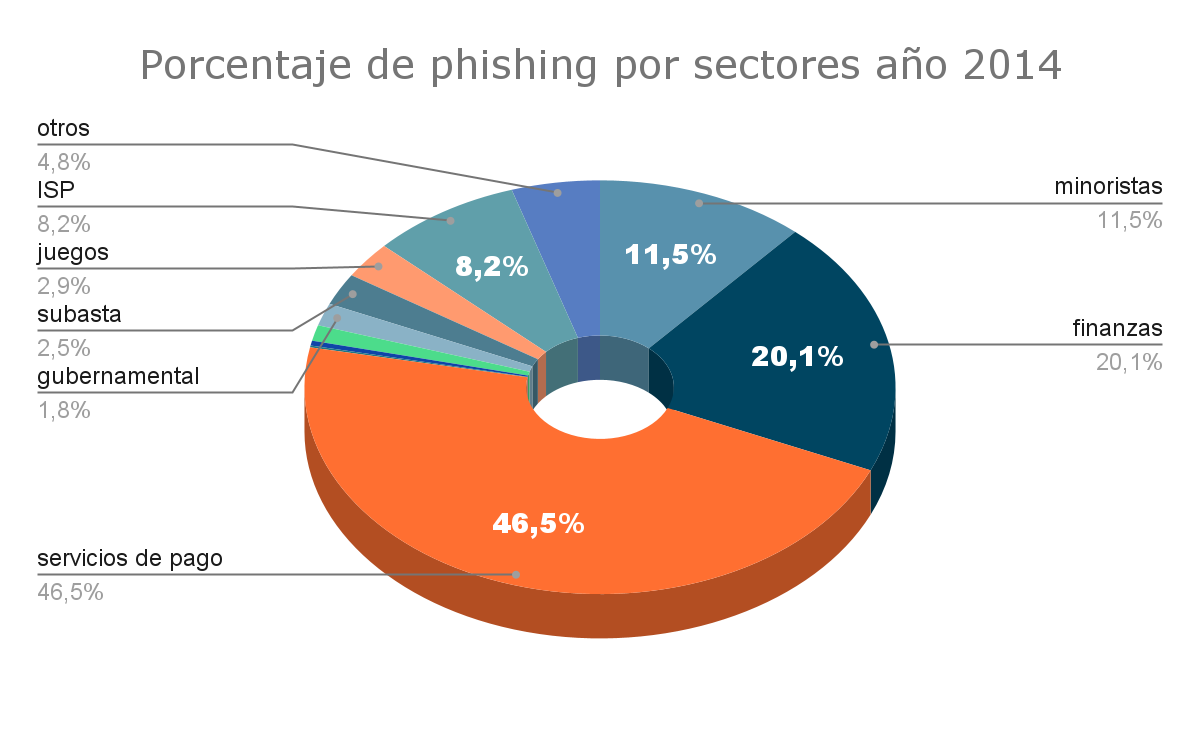
Las personas mayores no suelen usar estas aplicaciones bancarias que nos ayudan a dejar de transportar plata en efectivo, pero la mayoría que las usan no están conscientes de los problemas que lleva eso. En sus dispositivos móviles además usan las apps de redes sociales, que están repletas de personas, las cuales pueden mandar enlaces de páginas web maliciosas sin darse cuenta de lo ocurrido.

Vamos a ver unos porcentajes de las cantidades de ataques de phishing que sufren las compañías financieras, redes sociales y muchas otras. Según el reporte de la APWG(Anti-Phishing Working Group) en el año de 2004 el sector de la industria que sufrió más ataques de phishing son los Servicios Financieros que tiene un 40%, de cerca lo sigue por poco el sector minorista (principalmente minoristas en línea) con un 34%. El sector de los ISP(proveedores de servicios de internet) baja un poco, pero solo con el 25%. Por último los demás sectores se quedan con el 1%.



Ahora veamos cómo evolucionó luego de 10 años, en el año 2014, y cómo se sumaron nuevos sectores. Estos son los minoristas con 11.5% de los ataques de phishing bajando del 34% que tenían hace 10 años atrás, finanzas con el 20.1% que también bajó, servicios de pago con un 46.51% que ahora pasa a ser el mas problematico con casi la mitad de a cantidades de ataques, servicios de mensajería el 0.14% el más bajo de todos, clasificados 0.38%, redes sociales 1.23%, gubernamental 1.8%, subasta 2.5%, juegos 2.9%, ISP 8.2% que bajó de un 25% de hace diez años atrás, otros 4.8%.

Todos ellos, a la vista del gráfico, hace ver en donde se debería reforzar las seguridades, en donde deberíamos enfocarnos para concientizar a las personas de que no ingresen en URL falsos que les llegan por las casillas de correos electrónicos o por las redes sociales.

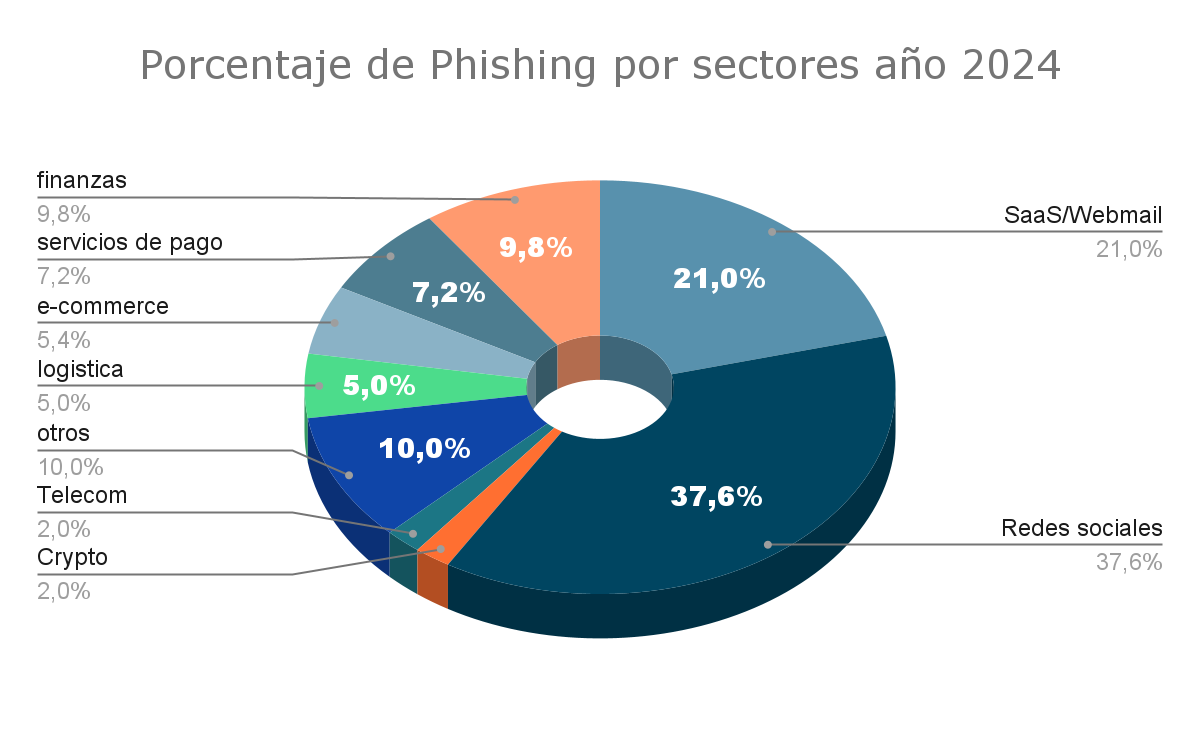


Recorramos 10 años más, hasta llegar a este año, el 2024, y aprendemos sobre la evolución de los ataques de phishing durante estos últimos 20 años.

Ahora vemos que en el primer trimestre de 2024, OpSec Security, miembro fundador de APWG, descubrió que las plataformas de redes sociales fueron el sector más atacado, representan continuó cayendo, del 24.9% de todos los ataques en el tercer trimestre de 2023 a 14% en el cuarto trimestre de 2023, a 9.8% en el primer trimestre de 2024. Ataques contra servicios de pago en línea como PayPal, Venmo, Stripe y empresas similares fueron otro 7,4% de todos los ataques.

"Las redes sociales cedieron algo de cuota de mercado a la industria de SaaS/Webmail, pero esos dos sectores aún representan casi el 60% de todo el phishing detectado", dijo Matthew Harris, Gerente Senior de Producto, Fraude en OpSec. "Hemos observado un mayor porcentaje de phishing dirigido a actividades que no requieren alta seguridad: menos hacia la banca y más hacia las cuentas de redes sociales, y Cuentas de Saas/Webmail como Microsoft Outlook y Netflix".

Harris también agregó: "Por último, y continuando con una tendencia que hemos visto durante los últimos 15 trimestres consecutivos, estamos una vez más con un registro de un fuerte aumento del fraude telefónico, con volúmenes de detección de vishing y smishing creciendo en más del 30 por ciento en comparación con el trimestre anterior".



Estas evidentes estadísticas nos muestran que las plataformas de redes sociales fueron el sector atacado con más frecuencia, atacados por el 37,4% de todos los ataques de phishing en el primer trimestre de 2024. El phishing en el segmento bancario continuó disminuyendo, hasta el 9,8 por ciento.

Evidentemente, las redes sociales, son ahora las más riesgosas a caer en el phishing, es por eso que las personas mayores son aún mucho más vulnerables a ser afectadas por este sistema de robo. Para no ser pescado por los delincuentes informáticos, nosotros, los usuarios finales, podemos utilizar herramientas de análisis de correos, que se comportan como filtro, listas negras de direcciones de sitios o incluso de remitentes, aplicaciones que analizan el flujo de información o hasta la detección de sitios clonados por su parecido visual.

En resumen de la sección, se muestran las recomendaciones detalladas.

Usuario:

1. Actitud de desconfianza hasta verificar la legitimidad.
2. Capacitarme.
   * Mantenerse actualizado
   * Reconocer una dirección de dominio web
   * Reconocer una dirección de email.
3. Atención a:
   * Mensajes de desconocidos.
   * Ofrecimiento de beneficios poco probables.
   * Solicitud de datos personales

Tomando como base toda esta información, existen dos caminos no excluyentes entre sí a seguir para combatir el avance de la cacería del phishing: avanzar en las herramientas que reducen significativamente la cantidad de ataques que nosotros los usuarios recibimos a diario y mejorar la concientización de todos nosotros para que logremos diferenciar mensajes legítimos de ataques con mejor tasa de éxito. Este trabajo se centra en el último de los dos caminos.

#### Reconocer una dirección de dominio web

Partamos de la recomendación de desconfiar de los mensajes recibidos y de los enlaces en sitios de Internet, para los usuarios sólo cabe inspeccionar cada sitio y determinar su veracidad, aspecto que fue cubierto por el estudio realizado.

Para poder detectar si un enlace es legítimo es necesario comprender dos aspectos: sus componentes y cómo se conforma una dirección web. Para ver la verdadera dirección web a la que apunta un enlace se debe poner el cursor encima de su contenido y el navegador mostrará en su parte inferior la dirección. A continuación mostraremos una representación de un dominio web con la estructura correcta, en la que se detallan sus componentes.

| **Protocolo** |  | **Dominio** |  |
| --- | --- | --- | --- |
| **https://docs.google.com/document/** | | | |
|  | **Sub Dominio** |  | **Página** |

##### Protocolo HTTPS

Protocolo de transferencia de hipertexto seguro (HTTPS) es una versión segura del protocolo HTTP que utiliza el SSL /TLS protocolo para cifrado y autenticación. HTTPS está especificado por RFC 2818 (Mayo de 2000) y utiliza el puerto 443 de forma predeterminada en lugar del puerto 80 de HTTP.

Mejor pasemos de la explicación técnica, a una clara, que cualquier persona pueda entender para poder aplicarla a su vida diaria.

El protocolo HTTPS hace posible que los usuarios del sitio web transmitan datos confidenciales como números de tarjetas de crédito, información bancaria y credenciales de inicio de sesión de forma segura a través de Internet. Por esta razón, HTTPS es especialmente importante para asegurar actividades en línea como compras, banca y trabajo remoto. Sin embargo, HTTPS se está convirtiendo rápidamente en el protocolo estándar para todos los sitios web, ya sea que intercambien o no datos confidenciales con los usuarios.

#### Evolución del phishing

Desde los primeros ataques de phishing hasta hoy, la realidad del uso de Internet cambió de forma considerable. Según el indicador “Individuos usando Internet (% de población)” medido por The World Bank , en 1995 menos del 1% de la población del mundo utiliza Internet. Desde el año 2014, este valor superó el 40% y continúa en aumento.

De la mano de este cambio de contexto de Internet, se advierte un crecimiento en la motivación para realizar ataques de phishing y, por lo tanto, resulta esperable observar un incremento de este tipo de actividad. Refleja la variación en la cantidad de sitios reportados con phishing detectados según los reportes de tendencia de Anti-phishing Working Group.

La evaluación de APWG es que la disponibilidad de muestras de voz y video de alta fidelidad en la Web, información personal íntima en las redes sociales y datos financieros personales vendidos en los mercados de la web oscura harán que sea cada vez más fácil para las bandas cibernéticas usar la IA para crear estafas excepcionalmente potentes.



En conjunto con el incremento en la cantidad, existe un proceso de perfeccionamiento en los aspectos técnicos del ataque, manteniéndose siempre estable el objetivo: lograr que uno o más usuarios entreguen información en forma inadvertida a una fuente no autorizada. Sin embargo, para mejorar la tasa de éxito y/o expandir los vectores de ataque, se desarrollaron nuevas técnicas, como las que se describen a continuación.

Phishing dirigido (en inglés spear phishing): en lugar de enviar grandes cantidades de mensajes con una pequeña probabilidad de respuesta, el atacante elige un objetivo (persona u organización), lo investiga y personaliza la comunicación. Esto dificulta que la víctima note que el mensaje es ilegítimo.

Inyección de contenido: es un ataque a los sitios web en el cual el atacante obtiene la capacidad de modificar parte del contenido de un sitio legítimo. Hasta aquí no se relaciona con el phishing, aunque se ha utilizado esta técnica para dirigir a los usuarios de un sitio legítimo a uno que no lo es.

Punycode: es un mecanismo para ampliar los caracteres permitidos en una dirección de un sitio web. En general, un buen mecanismo de defensa ante el phishing es revisar la dirección del sitio que uno está navegando; si no es la del sitio que se desea, probablemente se esté ante un ataque.

### Bibliografía

1. Based Frauds Allow Scammers to Engage with Victims More Personally.

###### <https://apwg.org/apwg-q1-report-phone-based-phishing-grows-explosively-shifting-the-cybercrime-threatscape/>

1. APWG Q4 Report Finds 2023 Was a Record Year for Phishing.

###### <https://apwg.org/apwg-q4-report-finds-2023-was-record-year-for-phishing/>

1. Phishing Activity Trends Report.

###### [https://docs.apwg.org/reports/apwg\_trends\_report\_q1\_2024.pdf?\_gl=1\*axbskb\*\_ga\*MTcxOTgwOTMuMTcyOTAzNjQ4Mw..\*\_ga\_55RF0RHXSR\*MTcyOTAzNjQ4My4xLjEuMTcyOTAzNjY1Mi4wLjAuMA](https://docs.apwg.org/reports/apwg_trends_report_q1_2024.pdf?_gl=1*axbskb*_ga*MTcxOTgwOTMuMTcyOTAzNjQ4Mw..*_ga_55RF0RHXSR*MTcyOTAzNjQ4My4xLjEuMTcyOTAzNjY1Mi4wLjAuMA)..

1. Reglamento general de protección de datos.

###### <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm>

1. ¿Qué es la ciberseguridad?

###### <https://aws.amazon.com/es/what-is/cybersecurity/>