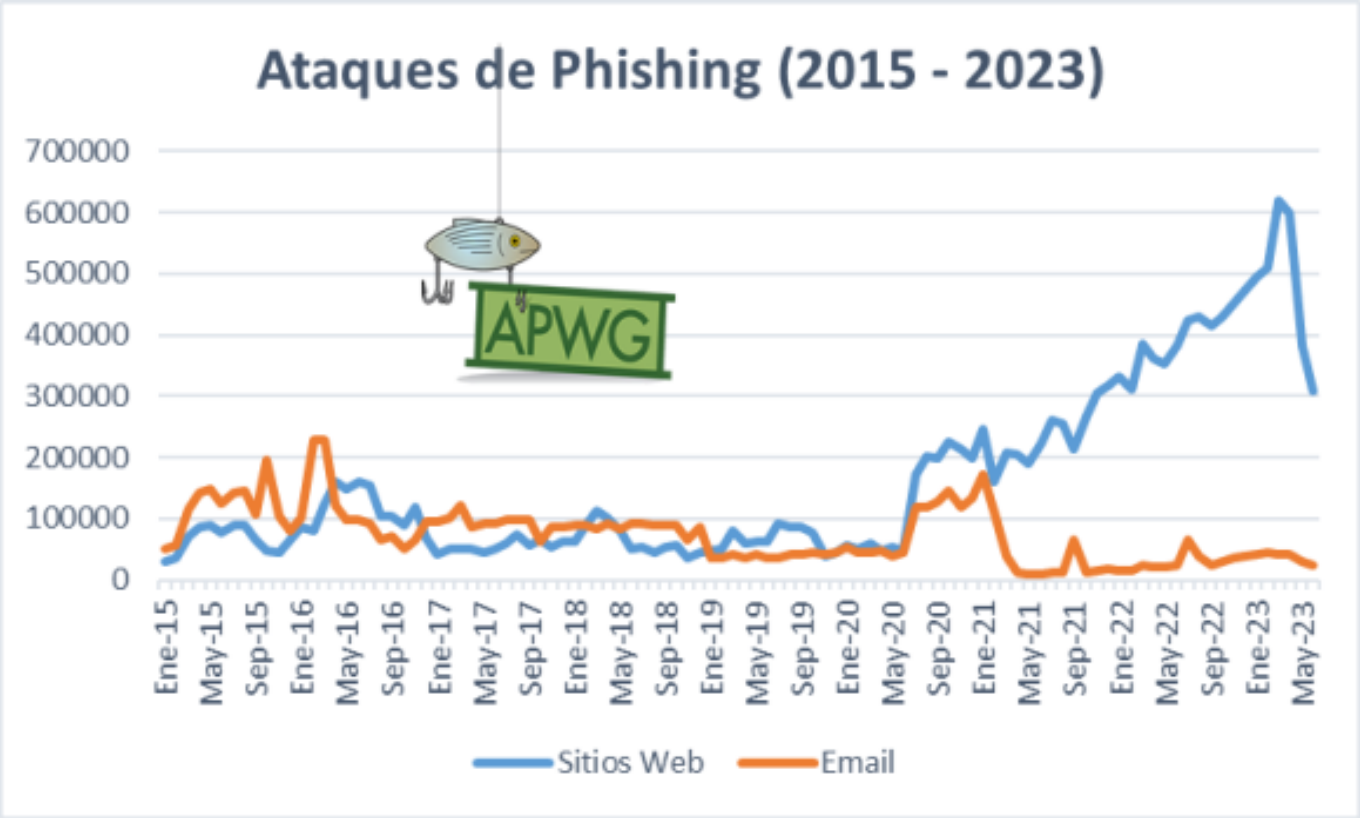
Hoy hablaremos sobre uno de los ataques muy conocidos en el ciberespacio, se trata de la suplantación de identidad o phishing, escenario que, después de casi tres décadas, continúa siendo utilizado para obtener de forma fraudulenta datos privados de los usuarios.

El Reporte Anual de Amenazas de Seguridad de Internet, emitido hace solo dos meses por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), así lo refleja y arroja que, en los últimos años, las tácticas más sencillas y los delincuentes informáticos más innovadores consiguieron resultados sin precedentes en el panorama de las amenazas mundiales. Por otra parte, este estudio hace referencia a como los ataques de phishing han seguido aumentando durante el año 2023, no solo en términos de vectores y números, sino también en términos de impacto.

Phoca PDF



La gran dependencia de la tecnología para la protección contra amenazas cibernéticas en constante evolución ignora muchas veces el elemento más crítico: el factor humano. Los ataques de phishing son uno de los más comunes entre los de ingeniería social, varios trabajos científicos y periodísticos así lo confirman. Según el Grupo de Trabajo Anti-phishing (APWG, según sus siglas en idioma inglés) estos emplean subterfugios técnicos y de ingeniería social para robar los datos de identidad personal y las credenciales de las cuentas financieras de los consumidores. Este tipo de ataque suele lanzarse principalmente a través de mensajes de correo electrónico, que parecen ser enviados desde una fuente acreditada, con la intención de persuadir al usuario de que abra un archivo adjunto malicioso o siga una dirección URL fraudulenta. El 65% del total de los ataques de phishing se realiza mediante el envío de hipervínculos maliciosos dentro del correo electrónico.

Por otra parte, estadísticas globales recientes ofrecidas por la compañía Cofense, una de las líderes en la gestión de amenazas de phishing según el cuadrante mágico de la empresa consultora Gartner en el presente año, afirman que entre los numerosos correos electrónicos sospechosos que puede recibir una empresa determinada, las tecnologías de filtrado de contenidos a menudo no analizan el objetivo con que se realizan estos ataques, lo cual puede ser considerado como una brecha de seguridad potencialmente costosa.

Phoca PDF

Cuba, que sigue apostando por la informatización de sus procesos y la transformación digital que consolide el progreso del país, no está ajena a esta realidad objetiva, y más teniendo en cuenta que desde el 2017 el 12% de los usuarios de Internet abre correos fraudulentos.

El sector de las comunicaciones y la ciberseguridad tienen un papel muy importante en el comercio electrónico, de cara al proceso de la bancarización. Hoy los más de 6.8 millones de cubanos que se conectan y que usan los pagos digitales a través de las plataformas como Transfermóvil y Enzona, pudieran en algún momento ser objeto de este tipo de ataques. Por lo tanto, acá las acostumbradas sugerencias:

Desde el sector empresarial:

- **Fijarse detenidamente en el emisor del mensaje:** La mayoría de los ataques de phishing contra el servicio de correo electrónico proviene de personas desconocidas. Se debe prestar especial atención por si existiese algo extraño en la dirección electrónica, como por ejemplo una “o” donde debería haber un cero, omisiones de letras o mal ordenadas (cubadbate.cu en lugar de cubadebate.cu, por ejemplo)
- **Nunca responda a ningún correo sospechoso:** Generalmente los *phisher* mantienen actualizado un registro de recepción y las respuestas a los mensajes que envían. Cuanto más responda, es probable que reciba más mensajes no deseados con el fin de capturar más información.
- **Piense bien antes de acceder a enlaces que soliciten cancelar una determinada suscripción o simplemente hacer clic en una dirección URL, aparentemente inofensiva:** Estos atacantes envían diversas cartas de cancelación de suscripción falsas, en su intento de recolectar direcciones de correo electrónico activas. No haga clic en los enlaces de los correos electrónicos que provengan de fuentes desconocidas.
- **Mantenga su navegador actualizado:** Asegúrese de utilizar la última versión de su navegador web y de que se hayan aplicado todos los últimos parches de seguridad de Internet.
- **Mantenga su antivirus actualizado:** Muchos antivirus como los desarrollados por las empresas Segurmática y Kaspersky presentan módulos de protección frente a amenazas web y frente a amenazas en el correo electrónico que puede resultar útiles en la detección de este tipo de ataques.

Desde lo personal:

- **Establezca una estrategia continua de auto entrenamiento:** Con esto se garantiza tener una formación especializada en cuanto al phishing, profundizando cada día en los conocimientos adquiridos

Phoca PDF

de los principales métodos de estafas. Existen varias herramientas automatizadas y comunidades interactivas en línea que proveen un mecanismo eficaz para aprender a reconocer estos ataques.

- **Sea escéptico:** Actúe con responsabilidad ante cualquier correo electrónico sospechoso. Antes de acceder a cualquier enlace o proceder a la descarga de cualquier archivo adjunto, revise las señales que pudieran indicar un presunto ataque. Si apareciera algún indicio de que una de esas señales se aplica al mensaje en cuestión, debe denunciarlo inmediatamente a los administradores y posteriormente proceda a borrarlo.
- **Confirme antes de ejecutar una acción:** Las empresas reales nunca proceden a solicitarle datos personales ya sea por correo electrónico o teléfono. No responda directamente a los correos electrónicos sospechosos. Comience siempre una nueva comunicación mediante los canales de atención oficiales de la empresa.
- **Verifique los certificados de seguridad:** No envíe ninguna información personal que no quisiera que tuviera un hacker salvo que esté convencido de que un sitio web es seguro. Verifique que la URL comienza con HTTPS y busque un icono de candado junto a la URL.
- **Cambie las contraseñas constantemente:** Los *phishers* no pueden hacer mucho con sus contraseñas si ya no son válidas. Actualice las contraseñas constantemente y emplee un administrador de contraseñas (***KeePass***, aplicación multiplataforma recomendada, en Apklis podrá encontrar su versión para dispositivos Android), para que su almacenamiento se realice de forma segura.
- **Realice chequeos periódicos a sus estados de cuentas bancarias:** Revise constantemente las últimas operaciones bancarias. Si no lo hace, podría pasar desapercibido algún un cargo extra fraudulento.

Por hoy es todo, hasta acá hemos compartido algunos de los consejos que pueden resultar útiles a la hora de protegernos ante un ataque de suplantación de identidad. Como siempre les recordamos mantener una actitud responsable en el ciberespacio.

Cubadebate.

Phoca PDF