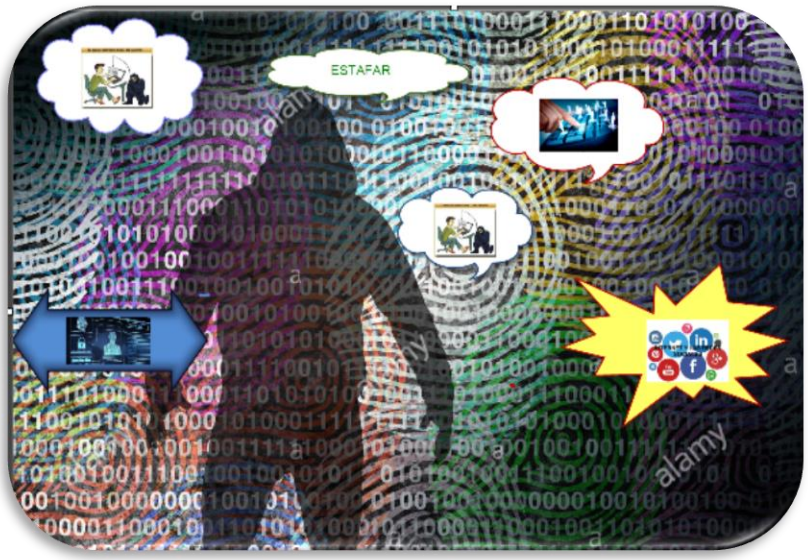
Boletín Informativo de Ciberseguridad

LAS ESTAFAS CIBERNÉTICAS EN LA ACTUALIDAD

Nivel de Importancia: ALTA (5)

Descripción:



La web se ha convertido en un arma de doble filo, nos brinda infinitos beneficios, pero, también es el medio ideal para novedosas formas de delinquir. Debemos mantenernos alertas l**os ciber-atacantes utilizan una amplia variedad de estrategias para acceder a un dispositivo o red, extorsionar o robar información valiosa.** Cuando se trata de comprender las amenazas actuales y cómo protegerse y proteger a una organización, conocer las diversas artimañas que buscan engañar a los usuarios ayuda a minimizar el impacto.

Las estadísticas de la Policía Nacional del Ecuador y la Fiscalía General del Estado, muestran qué en estos meses durante la pandemia, se incrementaron las denuncias de los ciudadanos, quienes aseguran haber sido víctimas de robos cibernéticos. Es así que las investigaciones muestran que una misma organización delictiva operaba desde Quito, Babahoyo y Santo Domingo, por lo que agentes desplegaron un operativo en esas ciudades y capturaron a seis personas. En la audiencia, se evidencio que esta red delictiva enviaba enlaces maliciosos a través de páginas de comercio electrónico. Cuando los afectados ingresaban al sitio web, un virus informático robaba sus datos personales o financieros. Con esta información, los sospechosos 'hackeaban' cuentas bancarias y sustraían fondos. En razón de que se elevó el uso de Internet para ejecutar transferencias bancarias.

Existen varios tipos de estafas realizados por Internet que debes evitar:

Estafas de Phishing

Estos ataques son muy comunes, tanto en redes corporativas como en las personales. Se llevan a cabo cuando un ciberdelincuente envía una comunicación (correo electrónico, llamada telefónica, mensaje de texto…) suplantando a otra persona, con el objetivo de extraer o acceder a credenciales, datos personales o información financiera.

Estafas de Spear Phishing

El spear phishing es mucho más sofisticado y dirigido. Los estafadores que practican este tipo de phishing investigan en profundidad a sus víctimas, así como la organización en la que trabaja, amigos, intereses, etc. para aumentar sus posibilidades de éxito.

Estafas de SMISHING

Es una nueva modalidad de cibercrimen, en base de técnicas mejoradas de ingeniería social con mensajes de texto dirigidos a los usuarios de telefonía móvil.

Boletín Informativo de Ciberseguridad

Los Ciberdelincuentes envían un SMS indicando sobre un supuesto grandioso premio económico, por parte de empresas y entidades legalmente constituidas, pero para ser reclamados, se requiere realizar recargas a números desconocidos o depositar cierta cantidad de dinero para los viáticos, así se concluye la estafa
Este tipo de mensajes de texto "Estafa" son enviado por los Ciberdelincuentes frecuentemente desde las cárceles, si usted recibe uno de ellos, por favor elimínelo inmediatamente.

Estafa a través de dispositivos móviles

Los dispositivos móviles están siendo cada vez más atacados por estafas criminales. Las aplicaciones falsas utilizadas para extraer datos o para pedir un rescate por recuperarlos (ransomware) están a la orden del día, especialmente para los sistemas operativos Android.

Estafas a través de Ingeniería Social (manipulación psicológica, intenta lograr que las demás personas hagan las cosas que se desea que hagan)

Buscan usuarios desprevenidos con el objetivo de que realicen una determinada acción, como descargar un virus o facilitar información personal a cambio de un software antivirus gratuito, películas que los usuarios pueden descargar, venas online, promociones atractivas, etc.; para que la víctima la instale en su ordenador. Si bien este tipo de estafas puede tomar muchas formas, la finalidad es siempre la misma: atraer a los usuarios para que instalen algo malicioso.

Recomendaciones:

- ✓ Mantenerse atento a los mensajes no solicitados: Si desconfía del emisor, no abra el mensaje ¿Le resulta sospechoso? Bórrelo.
- ✓ Discreción a la hora de facilitar información: Si los usuarios no estuvieran entregando voluntariamente datos personales a los ciberdelincuentes, el phishing no sería una estafa efectiva.
- ✓ Evitar escribir su email institucional en foros o en redes sociales, Ya que los spambot llamados "cazacorreos", recorren páginas web, foros, listas y plataformas sociales en busca de direcciones de correo electrónico, evite poner el símbolo @ para que los bots no puedan encontrarlo. Por ejemplo, "dante[at]corporacion.com"
- ✓ Evitar ofertas gratuitas: “sí parece demasiado bueno para ser verdad es más probable que sea una estafa”, antes de hacer compras vía web, investigue previamente el dominio para evitar riesgos;
- ✓ No comparta cadenas que le recomiendan que reenvíe mensajes para conseguir un objetivo X, ya que proporcionará la dirección de sus contactos para ser víctima de nuevos correos spam
- ✓ Mantener actualizado el navegador y aplicar los parches de seguridad de su ordenador.
- ✓ Nunca responda e-mails de SPAM, ya que con esto sólo estamos confirmando nuestra dirección.
- ✓ En caso de contar con un sistema Antispam, márcalos como SPAM los mensajes que así se consideren, para ayudar al sistema a mejorar el filtrado
- ✓ Utiliza la cuenta de correo institucional únicamente para uso laboral.
- ✓ Utilizar siempre contraseñas fuertes y cambiarlas con frecuencia.
- ✓ Evitar instalar cualquier cosa que proceda de una fuente desconocida: A menos que provenga directamente de una fuente en la que se confíe, una descarga desde la web conlleva un riesgo inherente de infectar un equipo.
- ✓ Usar WiFi seguro: Los espacios públicos y tiendas que ofrecen conexiones gratuitas de WiFi son lugares habituales para los ataques.

Boletín Informativo de Ciberseguridad

Referencias:

- Dirección Nacional de Tecnologías de la Información y Comunicación a través de la Sección de Ciberseguridad.
- Dirección Nacional de Policía Nacional e Investigaciones, a través de la Unidad Nacional del Ciberdelito.
- Fiscalía General del Estado, estadísticas