Cuáles son los ataques cibernéticos más comunes en el mundo y cómo prevenirlos

Las estrategias de **cibercriminales** para poder acceder a la información personal de los usuarios son variadas y ponen en peligro la seguridad financiera de personas que no tienen conocimiento sobre cómo protegerse de estos ataques.

Un reporte Appgate, compañía dedicada a brindar soluciones de ciberseguridad, indica que **4 tipos de fraude** son los más comunes en 2022, por lo que es necesario saber cómo se llevan a cabo y qué pueden hacer los usuarios para proteger su información y su dinero de cibercriminales.

Phishing

La estrategia de fraude más común usada por cibercriminales y consiste en **suplantar la identidad** de una institución o empresa confiable para que el usuario comparta voluntariamente su información. Según el reporte Fraud Beat 2022 de la compañía de

seguridad, esta modalidad representa el 80 % de los incidentes que se reportan antes las autoridades y es una de las más sofisticadas y realistas.

El phishing consiste en suplantar la identidad de una institución o empresa confiable para que el usuario comparta voluntariamente su información (Difusión)

Los datos presentados dan cuenta de que más de **80.000 personas** son víctimas de esta estafa y exponen datos valiosos como su información personal y corporativa.

El vicepresidente de ventas para Latinoamérica de Appgate, David López Agudelo, indica que existen variantes de este método de suplantación de identidad, como llamadas telefónicas (Vishing), intercambio o duplicación de tarjetas SIM, y hasta códigos QR.

Credenciales robadas

La información de acceso a diversas cuentas es un objetivo importante para

los cibercriminales. La obtención de estos datos implica el robo de dinero en el **100 % de los casos**. Según el reporte, el 61% de las fugas de datos tuvieron origen en credenciales vulneradas y el 25% de las fugas provinieron de estos datos robados

La obtención de contraseñas o claves de acceso implica el robo de dinero en el 100 % de los casos, por lo que es importante que los usuarios refuercen sus contraseñas y accesos. (TN)

Es recomendable que los usuarios establezcan **contraseñas diferentes** para sus cuentas o perfiles en internet y no las compartan con otras personas, es necesario usar métodos que **refuerzan la seguridad**, como la autenticación multifactor o la implementación de biometría del comportamiento.

Secuestro de datos

Conocido como Ransomware, los ataques de este estilo inician en un 20 % por casos de credenciales de acceso a cuentas que fueron comprometidas y es casi imposible recuperarse de estos casos de fraude.

De acuerdo a Cybersecurity Ventures, empresa investigadora en cibereconomía, la cifra promedio de pérdidas como producto de las fugas de datos fue de **$2.56 millones de dólares**, un 52% más a comparación del 2020.

El secuestro de datos o Ransomware ataca directamente al dinero de los usuarios y, al menos en el 20 % de las veces, involucra también el robo de credenciales de usuarios. (INCIBE)

Las estimaciones indican que, para el año 2031, el monto a nivel mundial será de aproximadamente **$265 mil millones** de dólares.

Ataques a dispositivos

Los cibercriminales también se han enfocado en los datos de los celulares o tablets. En estos casos, los ciberataques son en forma de aplicaciones móviles, mensajes SMS y códigos QR de origen fraudulento.

El 41 % de las empresas de telefonía han registrado un **incremento de este tipo de incidentes** por medio de estas modalidades, mientras que 23 % de ellas ha indicado

haber encontrado cuentas falsas intentando hacerse pasar por clientes.

Los mensajes SMS son usados también como una forma de atacar los celulares de los usuarios para robar su información.

David López indica que, “el auge de la banca móvil y el uso de aplicaciones P2P para compartir datos, han hecho que el número de malwares diseñados para estos dispositivos se mayor. De esta forma se han detectado **156.710 troyanos** de banca móvil solo en 2020?

Necesidad de protección

El Fraud Beat 2022 de Appgate indica que el 45% de las empresas consideran que se están quedando atrás ante las capacidades de los atacantes. Es por ello que algunas posibles soluciones en las que están dispuestas a invertir son Inteligencia Artificial y machine learning, autenticación multifactor, sistemas de detección y monitoreo de fraudes, y el Monitoreo de transacciones.

El 78% de compañías indicó que los controles antifraude son una de las características más deseadas para el cliente en las plataformas digitales

Además, López asegura que una forma eficiente para poder hacer frente a los métodos de cibercriminales es el de potenciar la infraestructura tecnológica y contar “ con un enfoque estratégico, alineando sus capacidades de prevención de fraude y educación de los empleados, colaboradores y consumidores”.

Fuente: Infobae