BILLETES FALSOS

La policía Nacional a través de trabajo de inteligencia, seguimiento ha realizado varias capturas exitosas de billetes falsos.
Pero recordemos que la calidad de impresión en el mundo se ha perfeccionado radicalmente.
Esto significa que ha mejorado la falsificación de billetes pero debemos estar cauto al percibir los billetes recuerden utilizar tacto y vista.
No se fijen del exceso de intanglio o alto relieve de la solapa de los ex presidentes, ni de mirarlo contra la luz para visualizar la denominada marca de agua; tampoco del hilo de seguridad donde a la luz se aprecian las letras borrosas twenty (20) o five (5), ni de las microfibrillas o pelusas de color. Como es lógico , nadie carga en su bolsillo una lupa "Hscb" para analizar la calidad de la microimpresión. Por lo general, a los billetes falsos los arrugan y después los estiran para engañar nuestro sentido del tacto.

Lo recomendable y práctico es estar alerta a la textura del papel billete. Los originales son de lino y algodón; los falsos son de simple papel que por lo general se deslizan con mayor rapidéz entre los dedos y son más delgados. Si tienen un negocio, usen lámpara ultravioleta para ver los billetes e incluso los cheques. Y lo más fácil mojarle con agua una punta y rasguñarlo si es papel se descompone en el acto.

Cuando les llegue un billete falso no "lo crucen a otro incauto", cumplan con el deber moral de entregarlo urgente al Banco Central e informar cómo lo recibieron; de esta manera se les facilita a las autoridades de control capturar a los falsificadores y minimizar el daño a la gente honesta. La responsabilidad de cada uno de nosotros forjara la seguridad de todos y mitigará el impacto del crimen organizado.

Lcdo. Gunnar Lundh
Ced 0910976802

¿Qué es el phishing?

El phising o robo de identidad es básicamente un tipo de estafa en línea, y los autores de estos fraudes, conocidos como ladrones de identidad, son artistas del engaño con conocimientos técnicos. Utilizan spam, sitios web falsos, software de actividades ilegales y otras técnicas con las que engañan a la gente para que divulguen información confidencial, como los datos de su tarjeta de crédito o de su cuenta bancaria. En cuanto capturan suficiente información de las víctimas, ellos mismos pueden utilizar los datos robados para estafarlas (por ejemplo: abren nuevas cuentas con el nombre de la víctima o agotan su cuenta bancaria), o bien pueden vender esta información en el mercado negro a buen precio.
En la mayoría de los casos, los phishers envían oleadas de correos electrónicos de spam, en ocasiones, hasta millones de mensajes. Cada uno de estos correos electrónicos contiene un mensaje que parece proceder de una empresa de confianza y bien conocida. Por lo general, en el mensaje aparece el logotipo y el nombre de la empresa, y suele intentar provocar una respuesta emocional a una crisis falsa. El mensaje, redactado en un lenguaje comercial que denota urgencia, suele solicitar la información personal del usuario. En algunas ocasiones, el correo electrónico dirige al destinatario a un sitio web falso. El sitio web, al igual que el correo electrónico, parece auténtico y en algunos casos se enmascara su URL para hacer que la dirección parezca real.

En el sitio web falso, se pide al visitante que proporcione información confidencial: números de la seguridad social, números de cuenta, contraseñas, etcétera. Dado que el correo electrónico y su correspondiente sitio web parecen legítimos, los phishers saben que por lo menos un pequeño número de destinatarios caerán en la trampa y enviarán sus datos.
Aunque es imposible conocer los índices de respuesta actuales a los ataques de phishing por parte de las víctimas, se cree que de un 1 a un 10% de los destinatarios caen en la trampa de una campaña de estafas "satisfactoria", con un índice de respuesta de un 5%, aproximadamente. Para que tengamos una idea más clara, se puede afirmar que las campañas de spam suelen obtener en promedio un índice de respuesta inferior a un 1%.

Durante el año 2005, los ataques de los phishers se hicieron mucho más complejos.
Comenzaron a utilizar software de actividades ilegales junto con sus sitios web falsos, y aprovecharon vulnerabilidades conocidas de los exploradores de Internet para infectar los equipos víctima. Esta tendencia significa que con tan sólo hacer clic en el vínculo de un correo electrónico de phishing que conduce a un sitio web falso, es posible robar la identidad del usuario, dado que el phisher ya no necesita que el usuario introduzca su información personal; el caballo de Troya o el software espía que se implanta en el equipo capturará esta información la próxima vez que el usuario visite el sitio web legítimo del banco o de otro servicio en línea. Durante el pasado año, este tipo de software de actividades ilegales se hizo más selectivo (para capturar solamente la información solicitada por el phisher) y más sigiloso gracias a los rootkits y a otras técnicas de ocultación que les permiten mantenerse ocultos en el interior de un sistema infectado.

Otro ejemplo de lo mucho que están avanzando los conocimientos y las habilidades de los grupos de phishing es la utilización de las fallas en los diseños de sitios web para hacer que sus ataques resulten más convincentes. Así, por ejemplo, una falla en el sitio web de IRS (el servicio de recaudación de impuestos de los EE. UU.) permitió que los phishers lograsen que sus páginas "señuelo" parecieran el sitio web auténtico del IRS, a pesar de que la víctima se dirigió directamente a un servidor web diferente, propiedad de los criminales. Éste es sólo uno de los muchos ejemplos que muestran el avance constante de las habilidades técnicas de los estafadores.