Cooperativa Policía Nacional

CONSEJOS DE **PREVENCIÓN**

INTERNET

Le brindamos una lista de las amenazas más frecuentes:

- **Phishing.-** Zonas que falsifican sitios corporativos legítimos con el objetivo de obtener información confidencial financiera, u otro tipo de información de los usuarios.
- **Bot.-** Aplicaciones relacionadas, que se han infiltrado en las computadoras de los usuarios con fines maliciosos, por ejemplo, acceso remoto o robo de información.
- **Keylogger.-** Programas que se ejecutan de fondo y registran todos los movimientos del teclado, y que pueden enviar dicha información posiblemente contraseñas o información confidencial a un tercero externo.
- **Software Malicioso.-** Diseñado por una persona externa para atacar o manipular la máquina o la red, ya sea para causar daño, utilizar información y recursos en forma no autorizada.
- **Spyware.-** Software utilizado para registrar e informar sobre la actividad de una computadora de escritorio sin el conocimiento del usuario, excluye hardware y cookies.
- **Pharming.-** Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.
- **Troyanos.-** Los troyanos son programas maliciosos que están disfrazados como algo atractivo que invitan al usuario a ejecutarlo ocultando un software malicioso. Este software puede tener un efecto inmediato y consecuencias indeseables, por ejemplo, borrar los archivos del usuario, instalar programas indeseables o maliciosos.

Cooperativa Policía Nacional

Para que sus transacciones estén siempre seguras, tenga en cuenta los siguientes consejos:

- Evita realizar transacciones en lugares públicos como cafés internet, universidades, redes wifi de hoteles, centros comerciales, etc.

- Utiliza en tus contraseñas letras mayúsculas, minúsculas, números, símbolos y cámbialas periódicamente.

- Para ingresar a la página de nuestra Cooperativa hazlo siempre digitando la siguiente dirección: www.cpn.fin.ec

- Verifica que en el navegador aparezca un candado cerrado, ya que este es un símbolo de que el sitio web es seguro. Si presionas click en el candado podrás confirmar la identidad de la página web.

- Verifica y confirma que la pantalla donde ingresas tu nombre de usuario y clave empiece siempre con https:\\

- Al finalizar tu transacción en nuestro espacio virtual asegúrate de cerrar la sesión.

- Utiliza un antivirus reconocido en el mercado y manténlo actualizado en tu computador.

- Recuerda que la CPN nunca te contactará para solicitar información confidencial como las contraseñas de tus cuentas, a través del teléfono, correo electrónico o cualquier otro medio.