NFÓRMATE UPZ 29 Boletín # 41 / Febrero 2024

SEGURIDAD INFORMATICA EN LA UPZ 29

Según los testimonios de la comunidad a los cuales se les realizo una encuesta con algunas preguntas acerca de la seguridad informática que pueden tener día a día en los casos cuando ellos pagan sus recibos por medio de plataformas, personas que compran cosas en paginas de internet.

La comunidad se siente intranquila con todos estos procesos que día a día la comunidad realiza, el principal proceso que la comunidad realiza es los pagos de sus servicios públicos y la preocupación de esta es que en muchos casos no les llega una notificación directa de que el pago fue de manera exitosa y en el momento ellos se confían de que sus recibos fueron pagos, pero al tiempo les llega una notificación de que aún no ha realizado el pago correspondiente a la fecha.

Una de las soluciones que algunas personas les dan e verificar que el sitio web en donde van a realizar sus transacciones sea seguro y venga de una fuente confiable, ya que muchas personas hackean estos links para poder engañar a la gente o darle una facilidad de pago, además de eso otra forma de que la comunidad es engañada es que por ayudarles a realizar los pagos les solicitan la clave de sus cuentas para que el proceso sea más rápido, les piden que coloquen las mismas contraseñas en todos los sitios y ellos por salir rápidamente de estas cuentas lo realizan sin tener en cuenta los riesgos que se pueden presentar al mismo tiempo.

Expertos en el tema nos dan varios tips para que la comunidad de la UPZ 29 y en general toda la gente del pais no caiga en la trampa de aquellas personas que las podremos denominar tramposas. Aquí puedes ver algunos de estos tips.

Navegador actualizado: Mantén tu navegador web actualizado para aprovechar las últimas funciones de seguridad.

Firewall y antivirus: Instala y actualiza regularmente un programa antivirus y un firewall en tu computadora para protegerte contra malware y amenazas en línea.

Contraseñas fuertes: Utiliza contraseñas seguras y únicas para tus cuentas en línea. Evita utilizar la misma contraseña en múltiples sitios web.

Verificación en dos pasos: Habilita la verificación en dos pasos siempre que sea posible. Esto añade una capa adicional de seguridad al requerir un código adicional además de la contraseña.

Monitorización de cuentas: Revisa regularmente tus estados de cuenta y transacciones para detectar cualquier actividad sospechosa. Notifica a tu institución financiera inmediatamente si encuentras algo inusual.

Evita Wi-Fi público: Evita realizar transacciones financieras en redes Wi-Fi públicas, ya que pueden ser menos seguras. En su lugar, utiliza una conexión segura y privada.

Compra en sitios confiables: Realiza tus compras en sitios web conocidos y de confianza. Verifica las opiniones de otros usuarios antes de realizar transacciones en sitios menos conocidos.

Actualizaciones de software: Mantén actualizado tu sistema operativo y cualquier software relacionado con pagos en línea para beneficiarte de las últimas actualizaciones de seguridad.

Educación sobre phishing: Aprende a reconocer intentos de phishing, donde los estafadores intentan engañarte para revelar información sensible. No hagas clic en enlaces sospechosos ni compartas información confidencial a través de correos electrónicos no solicitados.