Asunto: Consejos de ciberseguridad para ayudar a mantenerlos seguros en el ciberespacio

Estimados residentes de NYCHA:

En reconocimiento al Mes de la Concientización sobre la Ciberseguridad, nos gustaría presentarles alguna información que les ayudará a mantenerse seguros en el ciberespacio, en la casa y en el trabajo. ¡Gracias por ayudar a mantener nuestro mundo más seguro en el ciberespacio!

Ponga de su parte. #Sea inteligente en el ciberespacio.

La ciberseguridad es responsabilidad de todos. Usted puede poner de su parte reportando cualquier situación sospechosa, implementando prácticas de seguridad más fuertes y ayudando a crear conciencia.

Cómo ser inteligente en el ciberespacio

El año pasado, las brechas en seguridad causadas por ataques cibernéticos a empresas americanas aumentaron un 17 por ciento. Eso es 1.474 brechas llevadas a cabo exitosamente en todo el país. Los delincuentes informáticos o ciberdelincuentes no sólo usan la tecnología para robar información, también dependen del error humano y nuestra tendencia natural a compartir información sobre nuestras vidas.

Manténgase alerta: sólo se necesita hacer un error. Las brechas de datos pocas veces son el resultado de un jaqueo delictivo a través de la infraestructura de una organización. A menudo, comienzan con una sola vulnerabilidad. Una persona es engañada para que entregue su contraseña u otra información, y todos los datos a los que el usuario tiene acceso quedan expuestos. Esté siempre alerta a los fraudes electrónicos (phishing) y de ingeniería social. Be wary of unusual sources, do not click on unknown links, and report suspicious NYCHA-related messages immediately to phish@nycha.nyc.gov.

consejos simples para estar a salvo

1. **Si ve algo, diga algo.**

   Si nota algo inusual en las páginas web de NYCHA o en las solicitudes de NYCHA, por favor, repórtelo al Centro de Atención al Cliente de NYCHA (CCC) al 718-707-7771.

2. **La información comercial es información personal.** Muchos de nosotros manejamos datos en el trabajo que son sensibles. No tienen que ser números de tarjetas de crédito o de Seguro Social, pueden ser datos de cualquier empleado o cliente, especialmente cualquier cosa que pueda estar vinculada a una persona específica. No comparta los datos de la empresa con nadie fuera de su organización.

3. **Guarde las contraseñas de forma inteligente y segura.** Las contraseñas deben ser fáciles de recordar, pero difíciles de adivinar. Puede utilizar una frase o una serie de palabras, pero asegúrese de incluir suficientes elementos al azar para que nadie pueda adivinarlas. Recuerde, especialmente si trabaja desde su casa, mantener los rúteres (routers), las redes y los

dispositivos conectados configurados correctamente.

4. **Manténgase actualizado.** Asegúrese, periódicamente, de que su software esté actualizado con la última versión disponible. Asegúrese de tener activada la protección contra virus/programas malignos (malware) en todos los equipos que utilice para trabajar y realice un análisis de virus informáticos con regularidad.

5. **Ser inteligente en el ciberespacio no se detiene cuando termina el día de trabajo.** Las redes sociales son parte del conjunto de herramientas para el fraude. Los delincuentes pueden buscar información en Google, en Facebook, o en cualquier lugar en línea para obtener información sobre usted. Evite compartir información potencialmente sensible en las redes sociales o en cualquier otro lugar en línea, y nunca utilice las plataformas sociales para llevar a cabo negocios relacionados con el trabajo o intercambiar información sensible.

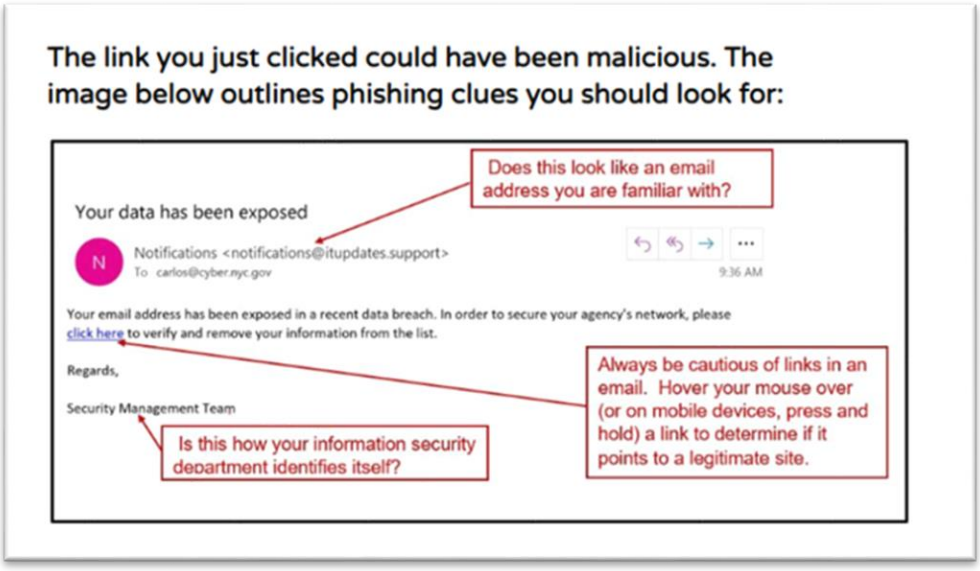
Para más información

Aprenda cómo #SerInteligenteenelCiberespacio viendo estos interesantes videos.

¿Qué es el fraude electrónico?

Los enlaces en el correo electrónico, los mensajes en las redes sociales, los textos y la publicidad en línea son a menudo las formas en que los ciberdelincuentes intentan robar su información personal. Incluso si conoce la fuente, si algo parece sospechoso, elimínelo. No haga clic en un enlace de un extraño. A continuación, se indican algunas formas de reconocer un intento de fraude electrónico:

Imagen: El enlace al que le acaba de hacer clic podría haber sido malicioso. la imagen de abajo muestra pistas de fraude electrónico (phishing) que debería buscar:



¿Qué es el Cibersecuestro de datos (Ransomware)?

El cibersecuestro de datos es un tipo de software malicioso, o programa maligno (malware), que le impide el acceso a los archivos, sistemas o redes de su equipo y exige el pago de un rescate para su devolución. Puede descargar un programa maligno de cibersecuestro de datos a una computadora sin saberlo abriendo un archivo adjunto de correo electrónico, haciendo clic en un anuncio, siguiendo un enlace o incluso visitando un sitio web que esté impregnado con un programa maligno. Una vez que se cargue en una computadora, bloqueará el acceso a la computadora o a los datos y archivos almacenados en ella. Por lo general, usted descubre que su equipo está infectado cuando ya no puede acceder a sus datos o ve mensajes informáticos que le informan sobre el ataque y le exigen el pago de un rescate.

La mejor manera de evitar el cibersecuestro de datos, o cualquier tipo de programa maligno, es ser un usuario de computadora cauteloso y meticuloso. Los distribuidores de programas malignos de computadoras se han vuelto cada vez más astutos, y ustedes deben tener cuidado con lo que descargan y en lo que hacen clic.

Gracias,

Greg Russ
Presidente y Director Ejecutivo General de NYCHA