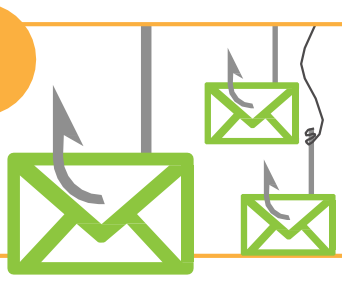
10 Tips para Trabajar desde Casa - SEGURAMENTE

1



Las estafas de Phishing son abundantes. Tenga en cuenta las estafas de Phishing dirigidas a trabajadores remotos con mensajes sensacionales o emocionales. Sin sus colegas cerca, debe estar mas atento a las estafas por correo electrónico y por teléfono. Reporte cualquier mensaje sospechoso a su equipo de seguridad de TI.

2

Tenga mucho cuidado con las noticias falsas y los sitios Web maliciosos que aprovechan los eventos de interés periodístico, como la pandemia COVID-19.

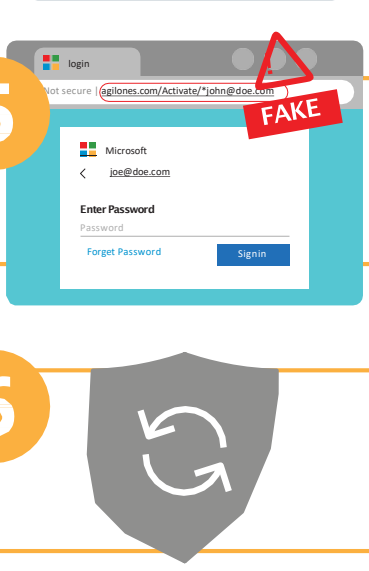
3

Tus passwords son la clave del reino. Sin la red de la compañía para protegerte, el poder recae directamente en sus manos o sus passwords. Asegúrese de que su password para cada sitio critico sea segura y única. Verifique la política sobre administradores de password y use uno si esta permitido.

4

Use Autenticación Multi-Factor siempre que sea posible. Esto es combinar su nombre de usuario y password con algo que posee, como una aplicación de contraseña única en su teléfono.

5

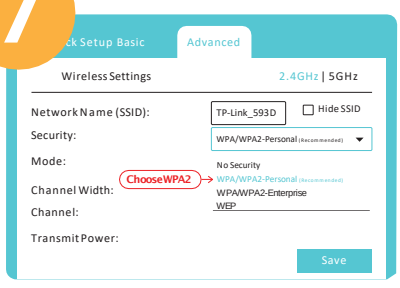


No caigas en ataques de "phishing para captura de passwords", donde los estafadores te engañan para que entregues tu nombre de usuario y passwords. Lo mejor es no hacer click en enlaces que te piden que actualices información. Mejor marque como favoritos los sitios que visita con frecuencia.

6

Aplica todas las características de Seguridad básicas. Mantenga su sistema operativo, complementos y software anti-virus actualizados y aplique parches de Seguridad cuando sea necesario.

7



Asegure la red WiFi de su hogar. Hay 2 cosas que debes hacer para configurar esto de forma Segura: Cambie el password por default del enrutador. Si todavía usa "admin/admin", "admin/password" o algo similar para iniciar sesión en su enrutador. Cambia esto.

Luego, cuando configure un password para su red WiFi, asegúrese de elegir WPA2 y hagas lo que hagas, no ejecutes una red wifi sin un password.

8

Mantenga un ambiente de trabajo privado. Mantenga el entorno de su hogar seguro y asegúrese que nadie tenga acceso a la computadora de su trabajo, incluidos su familia y sus hijos. Otros podrían descargar involuntariamente software malicioso o acceder a archivos que no deberían ver. Asegúrese de que sus conversaciones de trabajo permanezcan privadas y verifique su política en dispositivos domésticos inteligentes como Alexa o Google Home

Evite imprimir en casa, y si es necesario asegúrese de guardar los documentos confidenciales y triturarlos antes de desecharlos.

9

Usa una VPN. El uso de una red privada virtual (o VPN) proporciona un túnel seguros para todo su tráfico de internet, evitando que los delincuentes intercepten sus datos... Solicite a su equipo de Seguridad IT que configure una para usted.

10

Lee tus políticas. Están allí para mantenerlo a usted, a la empresa y a nuestros datos seguros. A su vez, esto le permite trabajar en la comodidad de sus PJ´s y zapatillas. Eres nuestra línea de defensa más fuerte, así que recuerda mantenerte súper vigilante.

Gracias por mantener su organización segura mientras trabaja de forma remota.