Trabajo remoto más seguro: Diez prácticas básicas de ciberseguridad para las Finanzas Inclusivas durante el CoVid-19 y después...

Introducción

La pandemia del CoVid-19 ha llevado a **muchas personas a trabajar desde el hogar repentinamente, para muchos por primera vez, y por una duración desconocida**. Aunque el trabajo remoto permite la continuidad de los negocios, puede que no exista un nivel apropiado de ciberseguridad en las infraestructuras, procesos, políticas y en la preparación de los empleados para enfrentar **riesgos cibernéticos cada vez más y más frecuentes y severos.**

El sector financiero a nivel global es uno de los objetivos principales para los piratas informáticos (hackers). Los piratas informáticos frecuentemente están organizados en redes criminales internacionales; tienen destrezas y herramientas avanzadas y están **buscando efectivo**. Las instituciones de inclusión financiera y sus amplias redes de agentes y servicios digitales emergentes tienen defensas más débiles que las de las instituciones más grandes. **Los empleados y los agentes** que usan dispositivos de la compañía o personales (PC, tableta y teléfono inteligente) desde ubicaciones dispersas para acceder al sistema bancario central o para la gestión de servicios financieros digitales y otras aplicaciones críticas de negocio son **canales excelentes para la intrusión**.

El **reciente aumento en los ataques con muchas estafas relacionadas con el COVID alrededor del mundo** ([1]) no debería enmascarar el hecho de que la inclusión financiera debe enfrentar un **desafío de ciberseguridad a largo plazo** con la proliferación de muchas técnicas que pueden estar mezcladas: ataques de suplantación de identidad (phishing), documentos maliciosos, sitios fraudulentos, suplantación de identidades de organizaciones gubernamentales e internacionales, Ransomware, ingeniería social, venta falsa de mascarillas, donaciones falsas a caridades… Mientras que algunos incidentes pueden estar limitados a los datos o las finanzas de los empleados, muchos pueden **poner en peligro a las mismas instituciones y la protección del cliente: pérdidas financieras, filtración de datos, discontinuidad del negocio, daños a la reputación.**

La primera línea de defensa será el comportamiento excepcional de los empleados. Este documento busca compartir las prácticas básicas de ciberseguridad cuya implementación es fácil y económica y que deben **aplicarse consistentemente en todos sus dispositivos.**

1. Copia de respaldo regular

- **Haga una copia de respaldo semanal** de sus documentos para protegerse contra la pérdida o el robo de su dispositivo, así como la corrupción o encriptación por parte de un software malicioso.
- La copia de respaldo debe incluir **todos sus documentos profesionales,** incluyendo correos electrónicos, contactos e imágenes.
- Haga la copia de respaldo en los servidores de la compañía, con un servicio de respaldo en línea, en un disco duro USB o en una memoria portátil USB.
- Desconecte el medio de respaldo móvil después de usarlo y almacénelo separadamente del dispositivo, en un lugar seguro.

[1] +667% en unas cuantas semanas, fuente Barracuda Networks, 26 de marzo de 2020

2. Fortalezca sus contraseñas

- **Cambie las contraseñas predeterminadas** ("0000", "admin", "1234", "password" para todos sus dispositivos, incluyendo el PIN de los teléfonos móviles.
- Use **contraseñas largas y complejas,** preferiblemente las contraseñas seguras recomendadas. Las paráfrasis son alternativas que se memorizan fácilmente. Por ejemplo: "¡Juan, ya es hora de trabajar!" se convertirá en "Jyehdt!".
- **Nunca comunique sus contraseñas** a nadie, ni por teléfono, ni correo electrónico, ni un formulario de un sitio web o una nota adhesiva en su pantalla.
- **Cambie** sus contraseñas regularmente.
- Use autenticación de dos factores o biométrica cuando sea posible.

✓ **CONSEJO:** Un software gratuito para la gestión de contraseñas le ayudará con esta tarea crítica.

3. Use software genuino, actualizado con la última versión disponible

- **Verifique la versión instalada** para cada dispositivo (computadora portátil, tablet, teléfono inteligente). Si no hay una versión reciente disponible para su dispositivo, como es el caso frecuentemente para los teléfonos inteligentes Android más antiguos, deje de utilizar este dispositivo para propósitos profesionales.
- **Use programas genuinos**: Los programas copiados ilegalmente frecuentemente han sido descargados de sitios web comprometidos. Descargue los programas únicamente de los sitios web oficiales de los editores con reputación.
- **Actualice sistemáticamente a la última versión**. Las actualizaciones que contienen arreglos de seguridad deben instalarse inmediatamente. Verifique que la opción de "actualización automática" esté seleccionada en la configuración de su sistema.

✓ **CONSEJO:** Existen equivalentes confiables y amplios que son de **Fuente Abierta (Open Source)** para la mayoría de programas, incluyendo paquetes de oficina (por ejemplo, LibreOffice).

4. Evite los ataques de suplantación de identidad (phishing)

- **Los correos electrónicos de suplantación de identidad** contienen **vínculos a sitios web comprometidos o documentos maliciosos** que activarán programas malignos si usted hace clic en ellos o los abre y eventualmente robarán sus credenciales. Esos correos electrónicos generalmente tienen las siguientes características:
    - **Suplantación**: el correo electrónico parece que ha sido enviado por una parte confiable (un banco, un operador de red, servicios gubernamentales, entidades de caridad, transportista), tanto en la dirección de correo electrónico del remitente como en el diseño del correo electrónico (logos de la compañía, texto).
    - **Sentido de urgencia:** para motivarle a activar el contenido ("usted ha recibido un premio o una donación", "Su cuenta está a punto de ser suspendida", "ofertas especiales", "verifique sus datos de cuenta bancaria", "factura urgente", "emergencia – envíe dinero a"...).
- **Al recibir un correo electrónico de un remitente inusual o con contenido sospechoso,** no abra el documento adjunto ni haga clic en el vínculo y **elimine el correo electrónico** inmediatamente. En caso de duda
    - **Verifique la dirección del remitente**: coloque el cursor sobre el nombre del remitente y se mostrará la dirección completa (puede variar entre los clientes del correo). La dirección puede ser de una persona real que se ha visto comprometida o de una dirección hecha para ese propósito, por ejemplo, @paypalinvoice
    - **Verifique el contenido** con su motor de búsqueda. Los fraudes frecuentemente son compartidos entre los expertos cibernéticos. Verifique la ortografía.

  - Si el correo parece ser legítimo, no haga clic en el vínculo, sino conéctese por medio de su navegador, ingresando la dirección completa, por ejemplo: www.paypal.com.
- ✓ **CONSEJO:** Su equipo de informática puede proporcionarle **apoyo adicional para verificar la validez y qué hacer en caso de que haya activado inadvertidamente el contenido malicioso.**

5. Navegación segura en la red

- **Manténgase alejado de sitios o aplicaciones que no tengan una reputación establecida**; frecuentemente están comprometidas (juegos, juegos de azar, copias de programas, descargas de música o video, contenido ilegal o de adultos).
- Esté extremadamente **atento al usar aplicaciones de pago y bancarias**, establezca límites de crédito bajos.
- Evite sitios en la red que usen protocolos http sin seguridad (los http**s** tienen seguridad).
- Cuide la información personal, profesional y su identidad digital, incluyendo las direcciones de correo electrónico.

6. Aseguro su acceso a la red Wi-Fi

- Establezca una **contraseña fuerte** para reemplazar la contraseña predeterminada de su direccionador (router) de Wi-Fi.
- Active un **protocolo fuerte (WPA2)** y desactive la Configuración Protegida de Wi-Fi (WPS).
- Cree una **cuenta de visitantes** para visitas, niños, etc. con derechos de acceso limitados.
- Nunca comparta sus credenciales.
- **Desactive el acceso remoto** al direccionador (router).
- Al viajar: evite usar redes públicas de Wi-Fi a menos que su organización proporcione una VPN (Virtual Private Network/Red Virtual Privada) para codificar la comunicación. En su lugar, utilice “hot spots” móviles 3G/4G.

7. Cuide todos sus dispositivos y sus datos

- **Instale un antivirus y active las actualizaciones automáticas**. Un antivirus no le protegerá de todo, pero es una base decente.
- **Nunca deje un dispositivo sin atender** en el hogar, la oficina o cuando viaje.
- Asegúrese de que las sesiones se cierren automáticamente después de unos cuantos minutos de estar ociosos.
- **No use una memoria portátil USB** para compartir datos. En su lugar, utilice transferencia de archivos segura en línea.
- **Proteja su lugar de trabajo**: asegúrese de que nadie observe su navegación por encima de su hombro. Nunca use computadoras públicas.
- ✓ **CONSEJO**: hay excelentes programas antivirus gratuitos.

8. Separe estrictamente el uso profesional del personal

- **Los dispositivos de la compañía** deben estar **dedicados a actividades profesionales,** no ser usados por parientes.
- **No instale ningún programa diferente a los que recomiende su equipo de informática.**
- **Cierre las aplicaciones o navegadores después de su uso**, en particular, el acceso a aplicaciones críticas del negocio.

9. No está solo

- **Póngase en contacto con su equipo de informática** para obtener ayuda para configurar sus dispositivos y el acceso a redes, para cualquier problema o actividad sospechosa o si cometió un error.
- **Póngase en contacto con las autoridades policiales** en caso de cualquier incidente.

Del lado de la compañía

10. Asegúrese de estar implementando rápidamente las medidas básicas de higiene cibernética para trabajar desde su hogar de forma segura

- **La concientización** es un componente clave de los sistemas de seguridad de la información.
- Provea un **punto de contacto y apoyo técnico** para los empleados (acceso, respaldo, programas antivirus, programas autorizados...).
- Configure un **acceso remoto VPN.**
- Establezca un lugar **central para compartir archivos con un proveedor de servicios en la nube**, con una estructura apropiada de carpetas, nombres de documentos y configuración del acceso.
- **Verifique y limite los derechos de acceso** para todos los empleados, incluyendo el equipo de informática.
- **Aplique parches de seguridad** para arreglar las vulnerabilidades conocidas.
- **Monitoree estrechamente los sistemas y las redes** en busca de comportamientos anormales.

Acerca de nosotros:

Suricate Solutions es una **compañía pionera de ciberseguridad para la inclusión financiera** con base en Luxemburgo y Senegal, donde gestiona el primer Centro de Operaciones de Ciberseguridad para la inclusión financiera. Es la afiliada para África de uno de los jugadores principales en Europa.

Debido a que en la actualidad los piratas cibernéticos tienen acceso virtualmente a cualquier sistema, Suricate se concentra especialmente en la seguridad operativa, la cual es la capacidad de **detectar, remediar y recuperarse de cualquier incidente de ciberseguridad** y, por lo tanto, fomenta la resiliencia cibernética. Diversos servicios están dirigidos a la inclusión financiera, por ejemplo, **supervisión de seguridad, detección de vulnerabilidades, pruebas de penetración, campañas de concientización, auditorías, asesoría y un "diagnóstico rápido de la ciberseguridad"** para evaluar la madurez de la organización e identificar las acciones prioritarias.

Para más información, póngase en contacto con: jlperrier (at) suricatesolutions (dot) com