Catholic Mutual..."CARES"

Estafas Cibernéticas Durante la Crisis del COVID-19

Los ciberdelincuentes están utilizando la crisis del COVID-19 como una oportunidad para aprovecharse de las personas, solicitando información personal o pidiendo donaciones para organizaciones benéficas y causas fraudulentas. Las personas deben estar conscientes de que existe una mayor exposición a estafas por correo electrónico y teléfono debido a la pandemia del COVID-19.

Además, deben tener cuidado cuando se trata de mensajes de texto y llamadas telefónicas relacionadas con el COVID-19.

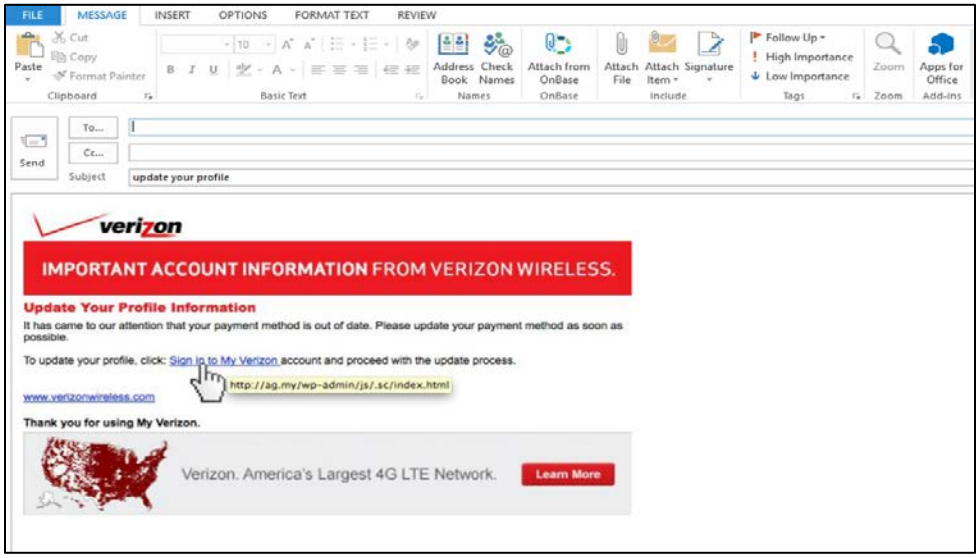
Catholic Mutual Group recomienda tomar las siguientes precauciones:

- Asegúrese de que haya planes actualizados de respuesta a incidentes y considere los cambios en el lugar de trabajo, como los empleados que trabajan de forma remota y utilizan dispositivos móviles para fines comerciales. Una mayor conciencia sobre la seguridad de la tecnología de la información es crítica.

- Manténgase alerta cuando revise correos electrónicos y llamadas telefónicas relacionadas con el COVID-19.

- No responda a solicitudes de información personal, ya sea por correo electrónico, teléfono o mensaje de texto. Si alguien solicita información personal a través de un correo electrónico o una llamada, elimine inmediatamente el correo electrónico o finalice la llamada. No proporcione información personal a menos que pueda verificar la identidad/autoridad de la fuente que solicita la información. Si cree que la solicitud es válida pero no puede verificar la identidad del solicitante, llame a la organización usted mismo para saber con seguridad con quién está hablando.

- Evite hacer clic en enlaces en correos electrónicos no solicitados y desconfíe de los archivos adjuntos de correo electrónico. Antes de hacer clic en cualquier enlace de un correo electrónico, desplace el ratón sobre el enlace y aparecerá la URL real. Asegúrese de que la URL esté vinculada a la dirección correcta. Los hackers a menudo falsifican la URL para que parezca una dirección legítima. Esta estafa a menudo es aplicada por *phishers* que utilizan compañías que son confiables, bien conocidas y que probablemente tengan grandes clientes consumidores (es decir, bancos, compañías de tarjetas de crédito, compañías de compras en línea e incluso su proveedor de telefonía inalámbrica, como se ilustra a continuación)



- Si recibe un correo electrónico que parece sospechoso, no copie y pegue ningún enlace en un navegador de búsqueda, reenvíe el correo electrónico sospechoso a otros o confíe únicamente en el software antivirus para detectarlo. Estas decisiones podrían dar como resultado que un delincuente cibernético obtenga acceso a su red poniendo en riesgo la información personal y confidencial.

- Al buscar educación y orientación sobre el COVID-19, solo use fuentes confiables/ legítimas, como sitios web del gobierno como CDC y sus departamentos de salud estatales/ locales para obtener información actualizada y basada en hechos.

- Puede ser solicitado por compañías o individuos con respecto a cualquier transacción relacionada con el COVID-19 (es decir, donaciones caritativas, limpieza, etc.) Incluso pueden ofrecerle donar fondos y solicitar su información de cuenta bancaria. NUNCA dé esta información. Incluso una fuente conocida que parece ser legítima podría, de hecho, ser fraudulenta. Una mejor práctica para protegerlo mejor de las estafas es que busque sus propias necesidades en lugar de aceptar solicitudes de fuentes con posibles estafas.

Si ocurre un incidente cibernético en su organización, notifique inmediatamente a su personal de TI. Para informar una reclamación durante el horario comercial, comuníquese con Jeff Schneider, Director de Reclamaciones de Catholic Mutual Group, al 800-228-6108 ext. 2404 (oficina) o 402-490-0021 (móvil). Durante el horario no comercial, comuníquese con nuestros expertos en seguros cibernéticos, Tokio Marine HCC, al 1-888-627-8995 y asegúrese de identificarse como miembro de Catholic Mutual.

Si necesita más ayuda durante este tiempo, no dude en ponerse en contacto con su representante de gestión de riesgos.

Además de las estafas cibernéticas mencionadas anteriormente, tenga en cuenta otras actividades fraudulentas que están ocurriendo. Si es una instalación que requiere el uso de las máscaras N-95, tenga en cuenta los productos fraudulentos que circulan actualmente. Vea el siguiente enlace, por ejemplo:

https://www.cdc.gov/niosh/npptl/usernotices/counterfeitResp.html