Auditoria

Normatividad

Global

Riesgo digital

Ciberseguridad en tiempos de Coronavirus

Al igual que las personas que llaman a su puerta diciendo que vienen del Ministerio a fumigar para luego robar, los cibercriminales están aprovechándose de la incertidumbre alrededor del coronavirus. Esté alerta a los emails de phishing (suplantación de identidad), links maliciosos y potenciales estafas. La policía británica ha emitido un alerta al público y estimó perdidas de 800 mil libras hasta ahora. La Oficina Nacional de Inteligencia contra el Fraude también ha emitido un alerta de estafas urgente.

Una oportunidad perfecto para la ingeniería social

Desafortunadamente, los cibercriminales siempre están esperando oportunidades como esta y usan la ingeniería social para explotar la debilidad humana, como cualquier otra vulnerabilidad. La ingeniería social es esencialmente manipulación social y una forma fácil para los criminales de obtener ingresos – y es altamente efectiva.

Las campañas de phishing de alto perfil relacionadas al coronavirus incluyen mails que parecen provenientes de los Centros de Prevención y Control de Enfermedades y la OMS – quienes emitieron guías sobre este tema. Los hackers también han atacado direcciones de email italianas, enviando documentos falsos que contienen el malware Trickbot.

A medida que esto progresa y las medidas gubernamentales se atrasan, estrategias más sofisticadas y específicas pueden surgir, como phishing relacionado a arreglos de continuidad del negocio.

Las firmas y los empleados deberían cuidarse de las casillas corporativas comprometidas – donde una dirección de email legitima se usa en forma fraudulenta. Esto puede ser particularmente convincente y el FBI anunció recientemente que esto le costó a las empresas e individuos americanos 1,7 mil millones de dólares en 2019.

Mirando mas allá del phishing, los cibercriminales pueden beneficiarse de la situación a través de links maliciosos o paginas falsas usando términos de búsqueda populares relacionados con el coronavirus para generar tráfico. Un reporte reciente de Webroot muestra que el 24% de todos los URLs malignos se encuentran en sitios legítimos, así que es importante seguir alerta aunque se este clickeando en una web de confianza.

Si desea más información o apoyo sobre cualquiera de los temas abordados por favor contáctenos.

Los asesores de Grant Thornton están enfocados en trabajar junto a nuestros clientes para apoyarlos en estos tiempos desafiantes de condiciones operativas críticas.

Roderick Marquis
Audit Partner
Grant Thornton Venezuela
E roderick.marquis@ve.gt.com

Jorge Gómez
Audit Partner
Grant Thornton Venezuela
E jorge.gomez@ve.gt.com

Carlos Diaz
Tax Partner
Grant Thornton Venezuela
E carlos.diaz@ve.gt.com

Grant Thornton

www.grantthornton.com.ve/