GUÍA DE CIBERSEGURIDAD

#asegúratedehacertuparte

¿QUÉ ESTÁ PASANDO?

"AUMENTO DE CIBERATAQUES DISFRAZADOS DE PREOCUPACIONES POR CORONAVIRUS"

Los ciberdelincuentes tienden a aprovecharse de temas de interés y alto flujo de búsqueda de información, lo cual lleva a una alta probabilidad que se descargue un archivo malicioso, con una apariencia de contenido de temas actuales.

La preocupación relacionada con el coronavirus y la proliferación de información ha llevado a un aumento significativo en los intentos de ataques cibernéticos: phishing, programas maliciosos y/o fraudes. Adicionalmente, nos vemos enfrentados a la desinformación debido a las noticias falsas, WhatsApp y redes sociales, son los medios más usados para difundir rumores, como por ejemplo testimonios de supuestos profesionales del sector salud que informan de noticias que los medios de comunicación no se atreven a contar.

¿QUE MOTIVA A UN CIBERDELINCUENTE?

1. Superar retos de ataques entre comunidades de ciberdelincuentes.
2. Identificar vulnerabilidades y explotarlas buscando un beneficio económico.
3. Lograr caos y confusión con un mensaje de contenido ideológico
4. Afectar la reputación de alguien y sacar beneficio de ello.

¿CÓMO ACTÚAN LOS CIBERDELINCUENTES?

Los ciberdelincuentes disponen de una variedad de programas informáticos y utilizan ingeniería social, como técnica de manipulación para obtener información de los propios usuarios, roban los datos para suplantar identidades, acceder a cuentas bancarias, redes sociales por medio de diferentes ataques. Su mayor ingreso es el mal uso de temas de moda y el error humano al manipular la información.

ALGUNOS TIPOS DE ATAQUES CIBERNÉTICOS COMUNES DURANTE ESTA ÉPOCA DE CRISIS

INGENIERÍA SOCIAL: Por medio de información confidencial que se obtiene a través de correos electrónicos y redes sociales manipulan a las personas.

MALWARE: Por medio de software malicioso, buscan tener un control total o parcial de los dispositivos y así chantajean a las personas.

PHISHING: Es uno de los fraudes más comunes en Internet, se lleva a cabo a través de la creación de páginas web falsas alterando el destinatario de los correos electrónicos.

EJEMPLOS DE CORREOS ELECTRÓNICOS RECIBIDOS EN ESTA ÉPOCA:

Con la alerta del coronavirus los ciberdelincuentes han visto la oportunidad de engañar a las personas para suplantar la identidad de industrias en especial relacionadas con el tema de atención médica, por ejemplo, se han suplantado destinatarios de la organización mundial de la salud (OMS).

EJEMPLOS DE LO QUE PODRÍAMOS RECIBIR EN NUESTRA BANDEJA DE ENTRADA:

1. Es probable que en la actualidad se puedan estar enviando correos que dicen tener la vacuna para el COVID 19, en donde es un supuesto medico quien redacta el correo y hay un enlace al final. Antes de acceder al enlace, valida su procedencia pasando el mouse por el link. Así podrás ver la página a la cual te direcciona.

Recuerda que los avances médicos los puedes consultar en las páginas oficiales de la OMS y/o de los entes gubernamentales en salud, todos estamos expuestos a una situación de alta incertidumbre en donde no hay entidades no gubernamentales que tengan de primera mano esta información.

2. Correos de centros de investigación: en su contenido puedes estar siendo invitado a participar en una investigación para desarrollar vacunas o medicamentos y para ingresar debes realizar un pago en monedas digitales y/o criptomonedas. Actualmente son los institutos educativos y del sector salud los responsables de estas investigaciones, si recibes un correo puedes verificar la participación a través de su página web, antes de realizar cualquier pago o de abrir un enlace.

¿CÓMO EVITARLO?

Te sugerimos las siguientes líneas de actuación:

CORREO ELECTRÓNICO:

Mantenerse alerta, evitar abrir correos sospechosos, no descargar ningún archivo adjunto ni hacer clic en ningún enlace donde no reconozcas el remitente, en especial aquellos que prometen contenido exclusivo, ten precaución de las descargas que realizas porque los archivos adjuntos aunque aparenten ser confiables, pueden tener inmersos virus informáticos que comprometen tu información.

BÚSQUEDA DE INFORMACIÓN:

Consulta fuentes oficiales y revisa los archivos a descargar.

MANTENER LA SALUD CIBERNÉTICA: Es tener cuidado con la información que llega y no reenviarla sin validar la veracidad de dicha información.

PROTEGE LA INFORMACIÓN: Realiza respaldo de tus datos frecuentemente para mantenerlos seguros.

RECOMENDACIONES:

- Realiza un respaldo frecuente de tus archivos para mantenerlos seguros.
- Ten cuidado con la información que recibes, no la reenvíes sin validar la veracidad de la misma.
- Consulta fuentes oficiales y revisa los archivos a descargar.
- El exceso de información puede llevar a una desinformación, confía en fuentes de organizaciones públicas y gubernamentales.
- #quedateencasa pensemos en colectivo, es momento de hacer un pare, volver a lo simple, tener momentos de dispersión y de control sobre lo digital.
- Estar en casa hace que cambien los hábitos, las interacciones y rutinas, es momento de reflexionar y de replantearnos nuevamente lo esencial y fluir con el cambio. Desconectarse es también estar conectado.
- Que la ansiedad por conocer no limite tu juicio y capacidad crítica, para reconocer destinatarios, fuentes y contenidos.
- No dudes en preguntar y consultar todas las dudas que tengas respecto a tu vida diaria en los diferentes medios de los sistemas de salud. Una buena decisión se centra en una buena fuente de información.
- Nos enfrentamos a un momento de alta incertidumbre, donde hay más preguntas que respuestas, es tiempo de comunicarnos entre los más cercanos y acudir a las fuentes gubernamentales para resolver las inquietudes.

- En este momento las compañías (aerolíneas, bancos, clínicas, supermercados), están usando sus redes sociales oficiales para comunicarse con sus clientes. Si tienes dudas con alguna en particular síguelas.
- Si recibes un correo electrónico sospechoso de una persona desconocida, elimínalo.
- Revisa el origen y el contenido de los correos electrónicos para identificar direcciones erróneas, dominios incorrectos (lo que hay después del @), URL con etiquetas engañosas (puedes verificarlo con .com, .org) y otras señales (idiomas del correo, nombre del remitente conocido).
- En caso de recibir un correo electrónico de un remitente desconocido y/o que tiene información que no esperabas, no lo abras y elimínalo inmediatamente. No respondas ni reenvíes correos sospechosos y reporta el fraude ante la entidad.
- Tener precaución con la ejecución o apertura de archivos adjuntos, especialmente si tienen la extensión .exe, .js o .xlsx.
- Recuerda que los corres de entidades financieras nunca te piden información de tu cuenta bancaria o claves de acceso a través de formularios web o un correo electrónico.
- Para evitar el robo de información de forma virtual, se debe mantener actualizado el sistema operativo, tener activado un antivirus licenciado, no abrir correos electrónicos sospechosos y evitar navegar por páginas inseguras.
- Para evitar el contacto físico, usa otros canales de comunicación tales como redes sociales, llamadas telefónicas, mensajes vía WhatsApp, si requieres hacer algún cambio o validación de estado de vuelos, reservas, citas médicas, exámenes médicos, domicilios, entre otros.
- En caso de que hayas abierto un correo fraudulento, te aconsejamos cambiar las contraseñas de todas tus cuentas desde otro dispositivo.

#asegúratedehacertuparte