DE LA RESPUESTA A LA CRISIS A LA TRANSFORMACIÓN

EL ROL DE LA DIGITALIZACIÓN EN LA PANDEMIA DE COVID-19 Y EN EL FUTURO

La pandemia de COVID-19 puso en evidencia la importancia de contar con una estrategia bien elaborada para el trabajo remoto. Decidimos compartir nuestra propia experiencia sobre el cambio en la modalidad de trabajo, ofreciendo asesoramiento para crear un entorno seguro. Esta guía les servirá de inspiración a todos los CISO, CIO y Gerentes de TI, así como a los CEO que deseen mantenerse informados, para descubrir la magia de la digitalización.

CYBERSECURITY
EXPERTS ON YOUR SIDE

Mayo de 2020

CONTENIDO

PARTE 1

CASO DE ÉXITO DE ESET:

Cómo superamos la pandemia de COVID-19 y lo que hemos aprendido de ella

La pandemia de COVID-19 fue una experiencia nueva para la humanidad y también para ESET. Aunque teníamos preparados planes de crisis, ninguno de ellos reflejó todos los desafíos que trajo la pandemia. Desde el comienzo, hubo claramente dos requisitos esenciales: mantener a nuestros empleados seguros y trabajar en forma remota para que el negocio siguiera funcionando. Así es como nos las arreglamos.

PARTE 1

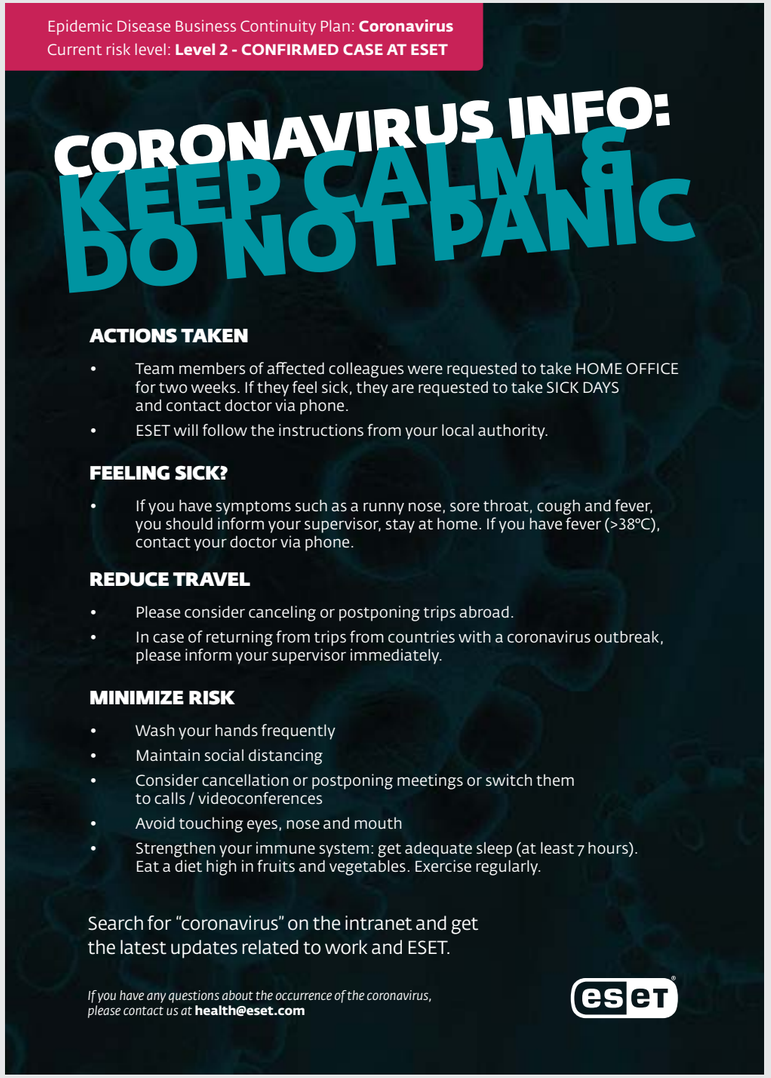
LA INFORMACIÓN EN PRIMER LUGAR

La falta de información genera problemas: al principio, muchos de nuestros colaboradores se asustaron. Apenas supimos que la situación se estaba agravando, pusimos a su disposición una dirección de correo electrónico exclusiva para que pudieran enviar preguntas en forma anónima.

Comenzamos a notar que los ellos buscaban activamente información sobre COVID-19. Vimos que en varias ocasiones consultaban fuentes poco confiables y descargaban archivos que podrían dañar sus computadoras. Por lo tanto, les facilitamos una lista de medios confiables y fuentes de expertos, y les recomendamos leer, por ejemplo, los estudios publicados por la Organización Mundial de la Salud (OMS) o la Universidad Johns Hopkins (JHU). Además, compartimos algunos consejos para ayudarlos a ser productivos en su trabajo desde casa y asesoramos a los gerentes sobre la administración de sus equipos en forma remota.

Dado que algunos de nuestros colaboradores no poseen dispositivos de la compañía, también hicimos carteles simples con todo tipo de información relevante, desde cómo lavarse las manos, hasta qué herramientas online usar y cómo pedir ayuda. Esta fue solo una de las medidas offline que implementamos.

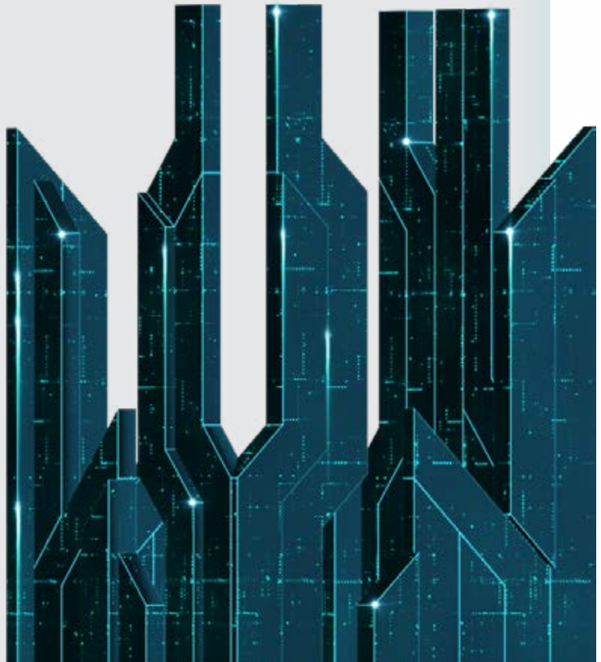
CARTELES PARA EMPLEADOS, CON MEDIDAS SOBRE LA PANDEMIA Y RECOMENDACIONES



PARTE 1

PLANIFICACIÓN, PLANIFICACIÓN Y MÁS PLANIFICACIÓN

Como la situación estaba empeorando gradualmente en todo el mundo, comenzamos a actualizar nuestro plan de continuidad empresarial en consonancia con la gripe pandémica. Teníamos algunos planes de respaldo del pasado, pero estaban desactualizados. En nuestro nuevo plan de crisis, tomamos en cuenta tres etapas diferentes.



ETAPA 1: MONITOREO

La primera etapa se aplicó cuando la pandemia ya estaba presente los países donde operan nuestras oficinas. Buscamos la forma de proteger a los colegas que se encontraban en viajes de negocios o que tenían viajes programados, y creamos, por ejemplo, una lista negra de países riesgosos. En el caso de las conferencias organizadas por ESET, pensamos programas alternativos de modo que se pudiera reemplazar a un orador enfermo a último momento.

ETAPA 2: USO LIMITADO DE LA OFICINA

La siguiente fase reflejó el momento en que anticipamos que podría haber un empleado infectado o que el gobierno podría proponer regulaciones que afectaran el trabajo de varios equipos. También comenzamos a ofrecer seminarios a través de la web con la participación de psicólogos. Nuestro departamento de Recursos Humanos desempeñó un papel crucial a este respecto.

ETAPA 3: CIERRE DE LA OFICINA

En la etapa final se tuvo en cuenta que podría haber una cuarentena forzada, o que la gerencia podría decidir que toda la empresa debería trabajar en forma remota, que es lo que realmente sucedió.

PARTE 1
PLANIFICACIÓN, PLANIFICACIÓN Y MÁS PLANIFICACIÓN

Al comienzo de la crisis, creamos un Comité de Salud, compuesto por cinco personas: el Gerente de Continuidad de Negocios de ESET, el Director de Recursos Humanos, nuestro Director de Operaciones, así como el Gerente de Soporte de TI y el Gerente de las Instalaciones. Su responsabilidad era monitorear la situación en forma periódica, hacer un seguimiento de los próximos pasos y comunicaciones, realizar evaluaciones de riesgos y ayudar a la alta gerencia a tomar decisiones importantes. En lo que respecta a nuestras oficinas internacionales, les recomendamos a los Directores de Recursos Humanos, los Gerentes de País y los Directores Regionales con quiénes debían tratar los impactos de estas decisiones, y les comunicamos que estaban obligados a informar al Comité de Salud.

También creamos reglas para viajar a otros países. En cuanto llegamos a la Etapa 2, cumplimos inmediatamente con las recomendaciones del Ministerio de Asuntos Exteriores de la República Eslovaca y les aconsejamos a nuestros colaboradores que no viajaran a ningún lado.

ASÍ ES COMO DANIEL CHROMEK, CISO DE ESET, ORGANIZÓ NUESTRO PLAN DE CONTINUIDAD EMPRESARIAL DURANTE LA PANDÉMIA Y ASEGURÓ LAS COMUNICACIONES INTERDEPARTAMENTALES.

ROL	RESPONSABILIDAD
COMITÉ DE SALUD 1. Gerente de Continuidad de Negocios, 2. Director de Recursos Humanos, 3. Director de Operaciones, 4. Gerente de Soporte de TI y 5. Gerente de las Instalaciones	Planificar la respuesta ante la crisis, preparar las comunicaciones, hacer un seguimiento de la situación, preparar la información necesaria para la toma de decisiones de la alta gerencia.
DIRECTOR DE RECURSOS HUMANOS EN LAS OFICINAS DE ESET	Comunicar a los colaboradores y manejar el brote en la oficina de ESET. Informar al Comité de Salud.
GERENTE DE PAÍS EN LAS OFICINAS DE ESET	Tomar decisiones acordes a su cargo en la alta gerencia. Decidir el cierre de la oficina y aprobar costos adicionales junto con: • el Director Regional y el Director de Negocios o el Director de Ventas para las oficinas de soporte y mantenimiento; • el Director de Tecnología o el Director de Arquitectura de Software para las oficinas de investigación y desarrollo.
DIRECTOR REGIONAL PARA LAS REGIONES DE EMEA, APAC, NORAM Y LATAM	Decidir el cierre de la oficina junto con el Gerente de País. Aprobar costos adicionales.

PARTE 1

LAS EMPRESAS DE TECNOLOGÍA TAMBIÉN PUEDEN TENER PROBLEMAS CON LA TECNOLOGÍA

Si bien nosotros no tuvimos ningún inconveniente con respecto a la seguridad, experimentamos problemas de organización.

Tan pronto como quedó claro que todos los empleados tendrían que trabajar de manera remota, tuvimos que conseguir computadoras portátiles adicionales para varios de ellos que hasta el momento trabajaban en equipos de escritorio, ya que no teníamos la cantidad suficiente disponible. Por lo tanto, nuestro equipo de TI tuvo que recorrer varios comercios para obtener todo lo que necesitábamos, lo que nos frenó un poco al principio. Al final, algunos de nuestros empleados terminaron llevándose a la casa la computadora de escritorio completa y otros accesorios. A continuación, hubo que configurar con rapidez todos los dispositivos nuevos; eventualmente, nuestros especialistas de TI lo lograron en tres días, durante una larga jornada de trabajo de fin de semana. **Lección aprendida: siempre verifique si tiene todos los equipos necesarios para el trabajo remoto.**

Con eso resuelto, nos dimos cuenta de que tampoco teníamos suficientes licencias de VPN para que todos nuestros empleados se conectaran a los sistemas internos desde su hogar. Desafortunadamente, nuestros proveedores estaban con dificultades para cubrir la gran demanda y demoraron mucho más tiempo del esperado para brindarnos los servicios requeridos. Esto demuestra claramente que por más que se esfuerce para crear el mejor plan de crisis, todo puede fallar si uno de los proveedores de los que depende su empresa no es capaz de suministrarle los servicios necesarios.

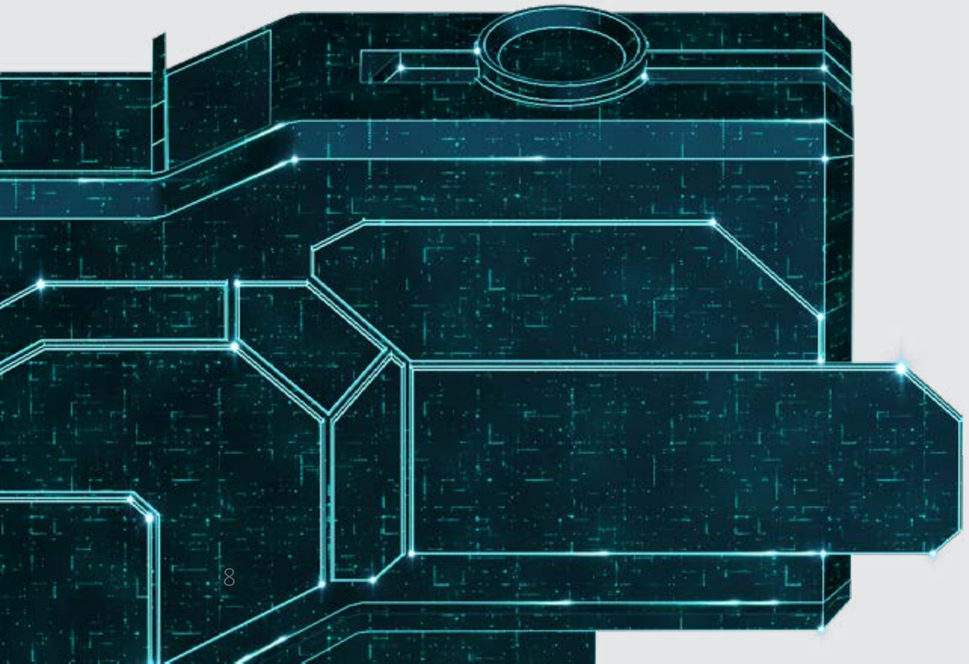
Daniel Chromek, CISO de ESET

De un momento a otro, la gravedad de la situación escaló y el 80% de nuestros empleados necesitaban acceso remoto... Había que cifrar todos los discos rígidos de los equipos de escritorio y preparar rápidamente las nuevas computadoras portátiles, lo que era una tarea muy demandante.

PARTE 1

LA SEGURIDAD PRIMERO

Fuera de la red corporativa, los dispositivos son más vulnerables a los ataques cibernéticos. Para poder mantener seguros tanto los dispositivos como los datos, nos centramos en capas de seguridad adicionales vitales para la protección de las endpoints y la seguridad del correo electrónico, desde el cifrado de disco completo y la autenticación en varias fases hasta la tecnología con modo sandbox en la nube.



SOLUCIONES DE SEGURIDAD QUE UTILIZAMOS DURANTE LA CRISIS

ESET Endpoint Security 7: plataforma de protección para endpoints que combina una sólida prevención contra malware, exploits y ransomware con los beneficios del machine learning.

ESET Dynamic Threat Defense: tecnología con sandboxing en la nube que emplea modelos de machine learning para detectar y analizar amenazas en las endpoints y los archivos adjuntos en e-mails; además detecta amenazas 0-day y ransomware.

ESET Security Management Center: consola de administración que permite controlar desde una única pantalla las capas de prevención, detección y respuesta de la seguridad para endpoints en todas las plataformas: equipos de escritorio, servidores, máquinas virtuales sin agente y dispositivos móviles.

ESET Secure Authentication: Una forma efectiva de implementar la autenticación en varias fases, diseñada para operar con todos los teléfonos, los tokens de hardware, las VPN y los servicios en la nube; con una función de autenticación impulsada.

Cifrado de disco completo de ESET: potente cifrado administrado en forma nativa por las consolas de administración remota de ESET, que aumenta la seguridad de los datos de las organizaciones para cumplir con las normativas vigentes.

MÁS INFORMACIÓN SOBRE CÓMO PROTEGER A SUS TRABAJADORES REMOTOS.

PARTE 1

LA CRISIS COMO CATALIZADOR

A pesar de causar muchos problemas, la crisis hizo que nos centremos en nuevos procesos y soluciones, que confiamos nos ayudarán en el futuro. Finalmente comenzamos a usar firmas electrónicas, alcanzamos la madurez en nuestros procesos de contratación online y mejoramos nuestra capacidad de administración remota. No solo aprendimos a trabajar remotamente sin tener que cancelar un solo proyecto importante, sino también a ser más productivos. Esto sin duda nos ayudará en el largo plazo.

Incluso antes de la crisis, sabíamos que nuestros empleados anhelaban tener más flexibilidad y la situación nos ayudó a satisfacer sus necesidades. Creemos que un lugar de trabajo totalmente digitalizado es el futuro y, gracias a la pandemia, dimos varios pasos en esa dirección.

LÍNEA DE TIEMPO: NUESTRA RESPUESTA A LA CRISIS A LO LARGO DEL TIEMPO

ENERO

CANTIDAD DE ARCHIVOS DE MALWARE INFORMADOS Y BORRADOS DE OUTLOOK: 6

1 DE ENERO

ETAPA 1: SEGUIMIENTO DE CANTIDAD DE PERSONAS EN LAS OFICINAS DE ESLOVAQUIA: 800

4 DE FEBRERO

CONFIGURACIÓN DE UN CORREO ELECTRÓNICO EXCLUSIVO PARA ASISTENCIA

10 DE MARZO

CREACIÓN DEL COMITÉ DE SALUD

12 DE MARZO

ETAPA 2: LIMITACIÓN DEL USO DE LA OFICINA

15 DE MARZO

ETAPA 3: CIERRE DE LA OFICINA

16 DE MARZO

ADQUISICIÓN DE LOS DISPOSITIVOS NECESARIOS

18 DE MARZO

CONFIGURACIÓN FINALIZADA DE LOS DISPOSITIVOS NUEVOS

ABRIL

CANTIDAD DE ARCHIVOS DE MALWARE INFORMADOS Y BORRADOS DE OUTLOOK: 27

10 DE ABRIL

MAYORÍA DE LOS EMPLEADOS TRABAJAN REMOTO. PERSONAS EN LAS OFICINAS DE ESLOVAQUIA: 25

PARTE 2
NUEVAS AMENAZAS EN JUEGO

¿Dónde están la ética y los valores? Lamentablemente, no significan nada para los ciberdelincuentes. Las crisis son ocasiones ideales para lanzar nuevos ataques. Aprovechan que los empleados están estresados, ansiosos y trabajan bajo presión, y que las empresas están introduciendo medidas nuevas en forma apresurada para sobrevivir. "*Los delincuentes aprovecharon rápidamente las oportunidades para obtener beneficios de esta crisis y adaptaron sus modos de operación o desarrollaron nuevas actividades criminales*", explica Catherine de Bolle, Directora Ejecutiva de Europol, en una guía publicada recientemente.

Nuestras propias experiencias lo han confirmado. Estamos recibiendo el doble de correos electrónicos de phishing de lo normal. Algunos de los remitentes incluso han estado utilizando nombres y contactos de empleados reales de ESET, y les piden a los destinatarios que paguen facturas fraudulentas, realicen determinadas tareas o compartan los detalles de su cuenta bancaria.

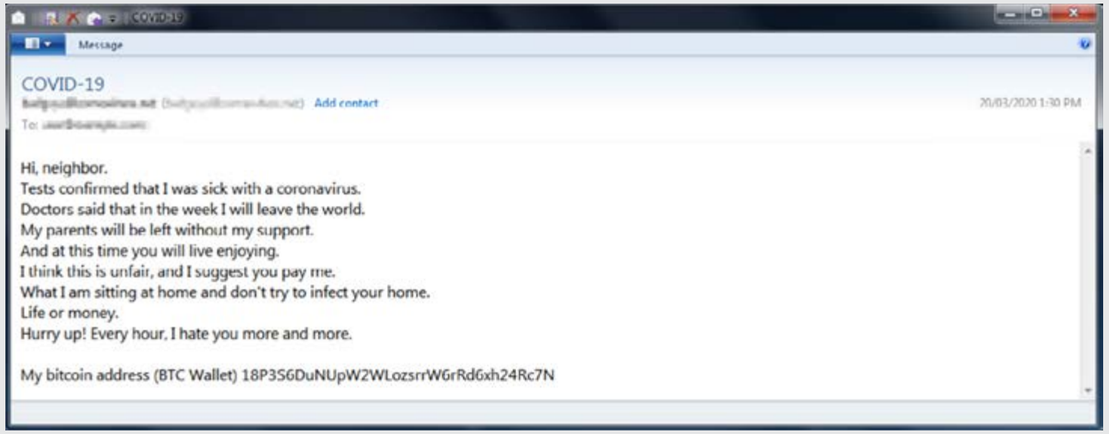
PARTE 2
AMENAZAS WEB

El tema del coronavirus se ha utilizado como señuelo en múltiples amenazas web. De acuerdo con el Informe de amenazas de ESET del primer trimestre de 2020, la cantidad de sitios web fraudulentos bloqueados aumentó en un 21% en comparación con el cuarto trimestre de 2019.

Los ciberdelincuentes, por ejemplo, han aprovechado la gran demanda de equipos y suministros médicos y fundaron tiendas electrónicas falsas para venderlos. Los sitios permiten procesar los pagos, pero los usuarios nunca reciben el pedido o reciben productos de calidad inferior. Según Europol, las autoridades de todo el mundo confiscaron alrededor de 34.000 máscaras quirúrgicas falsas solamente entre el 3 y el 10 de marzo de 2020. Con todos estos hechos que evidencian el aumento de los ataques, ESET se enfocó aún más en la concientización del personal mediante comunicaciones periódicas donde se les informa a los empleados sobre las amenazas y las estafas actuales.

Los ciberdelincuentes hasta llegaron a amenazar a los destinatarios de sus e-mails con infectarlos a ellos y a sus familias con coronavirus si se negaban a pagar el rescate solicitado. Además, aumentaron los ataques a los e-mails comerciales, por lo que las empresas ahora deben lidiar con una cantidad aún mayor de ataques de ransomware y malware.

CORREOS ELECTRÓNICOS DE ESTAFAS DE EXTORSIÓN SOBRE EL CORONAVIRUS



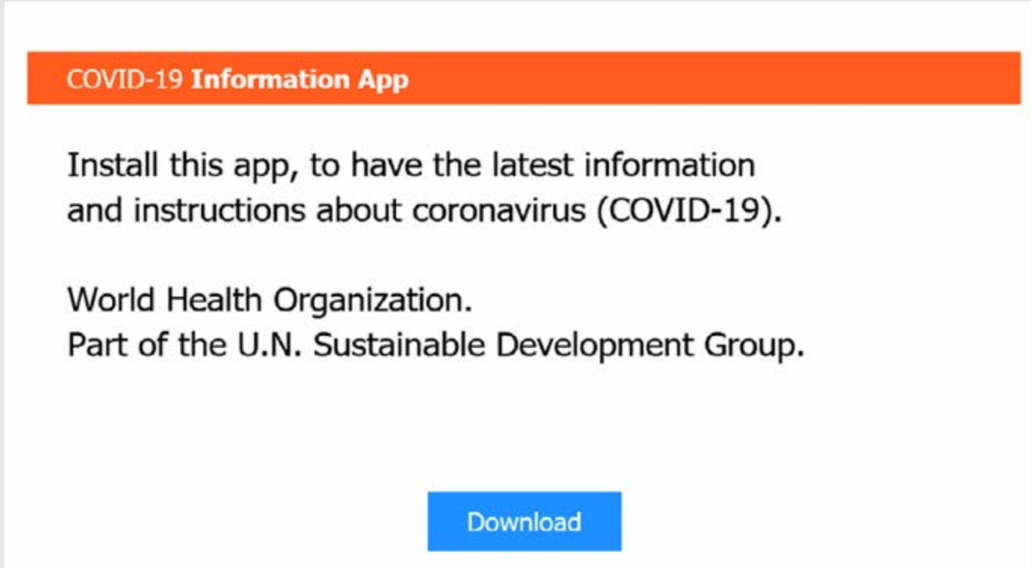
MÁS INFORMACIÓN SOBRE CÓMO LAS ESTAFAS APROVECHAN EL MIEDO AL CORONAVIRUS Y LOS DESAFÍOS DIGITALES QUE TRAJO.

PARTE 2
AUTORIDADES FALSAS

Los empleados de ESET no fueron los únicos que depositaron su confianza en la OMS. Lamentablemente, esta organización fue una de las más suplantadas en las campañas de estafadores y se convirtió en una puerta a través de la cual los atacantes difunden noticias falsas, pretenden tener información importante y les piden a los usuarios que hagan clic en enlaces maliciosos, por ejemplo, para robarles datos personales.

> *Los atacantes aprovechan el hecho de que las personas están nerviosas y trabajan desde casa.*
>
> **Daniel Chromek, CISO de ESET**

SITIO WEB MALICIOSO QUE SE HACE PASAR POR LA OMS Y QUE ENGAÑA A LOS USUARIOS PARA QUE DESCARGUEN MALWARE.

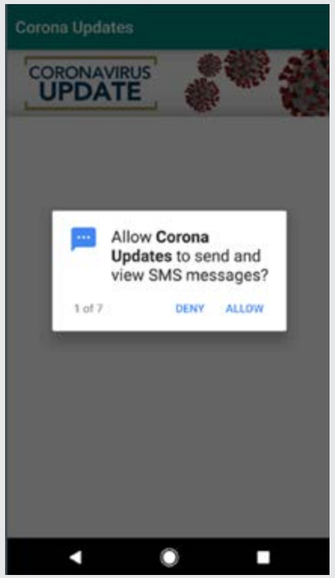


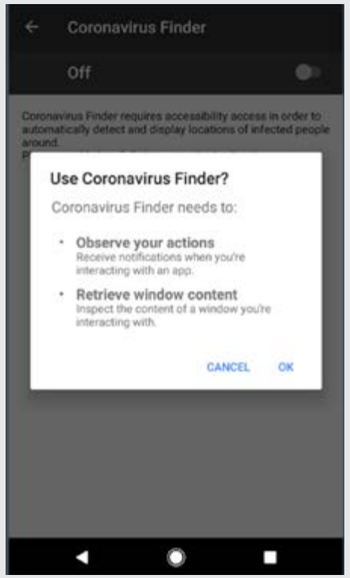
PARTE 2

APLICACIONES PELIGROSAS

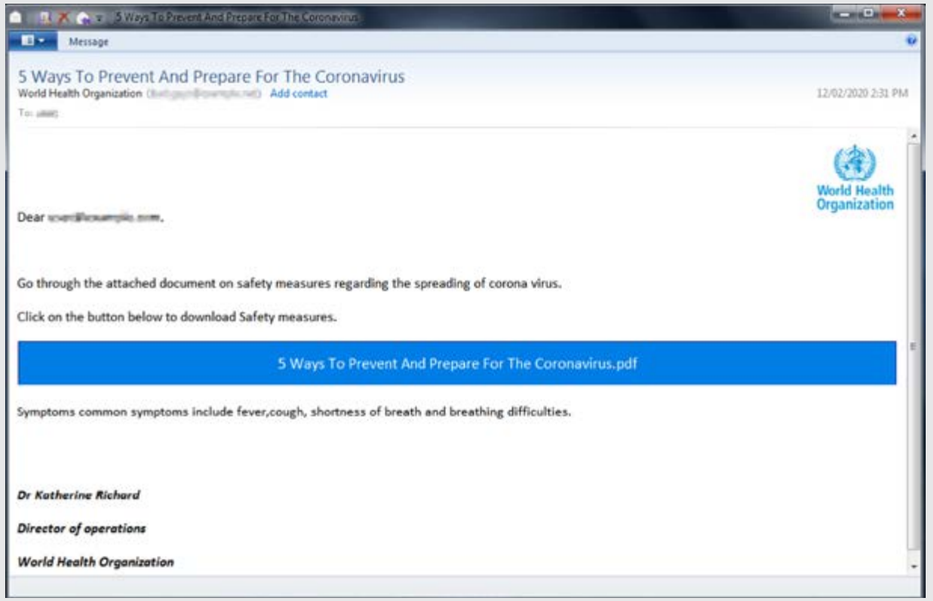
Además, aparecieron nuevas aplicaciones maliciosas que supuestamente les permiten a los usuarios identificar síntomas, rastrear los contactos o generar compensaciones financieras. Sin embargo, muchas de esas aplicaciones no son más que familias de troyanos bancarios, ransomware, spyware y adware.

EJEMPLOS DE MALWARE DE TEMAS RELACIONADOS AL CORONAVIRUS QUE SOLICITA PERMISOS EN ANDROID.





CORREO ELECTRÓNICO DE SPAM QUE SE HACE PASAR POR LA OMS.



FUENTES DE IMÁGENES: INFORME DE AMENAZAS DE ESET 2020

PARTE 2

ATAQUES CIBERNÉTICOS SOBRE COVID-19 EN NÚMEROS

- Google detectó 18 millones de correos electrónicos diarios de malware y phishing relacionados con COVID-19 en la segunda semana de abril de 2020. En promedio, Google bloquea más de 100 millones de correos electrónicos de phishing por día.*

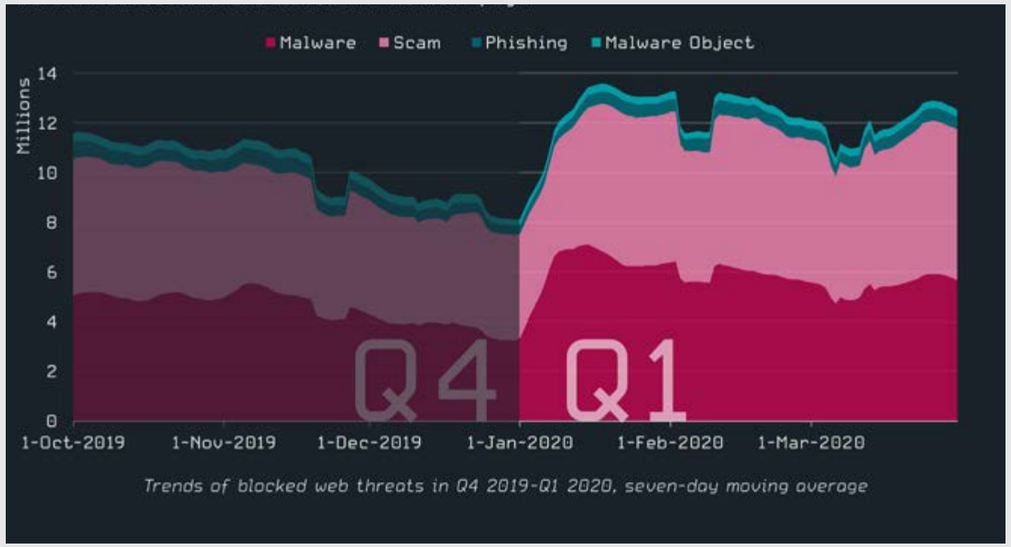
- Google detectó 240 millones de mensajes diarios de spam relacionados con COVID-19 durante el pico de COVID-19.

- El crecimiento registrado de los correos electrónicos de phishing relacionados con COVID-19 medidos en todo el mundo durante el primer trimestre de 2020 fue de 600%, según la investigación de KnowBe4.

* *ESET es miembro fundador de la App Defense Alliance para proteger la tienda Google Play Store y ofrece sus multipremiadas capacidades de detección y seguridad mejoradas para el ecosistema de Android. ESET además protege a los usuarios de Google Chrome a través del motor de ESET integrado en Google Chrome Cleanup, una herramienta de seguridad que alerta a los usuarios de Google Chrome sobre posibles amenazas. ESET también tiene una integración con Chronicle, que es una división de Google Cloud.*

Más información sobre la cooperación de ESET con Google.

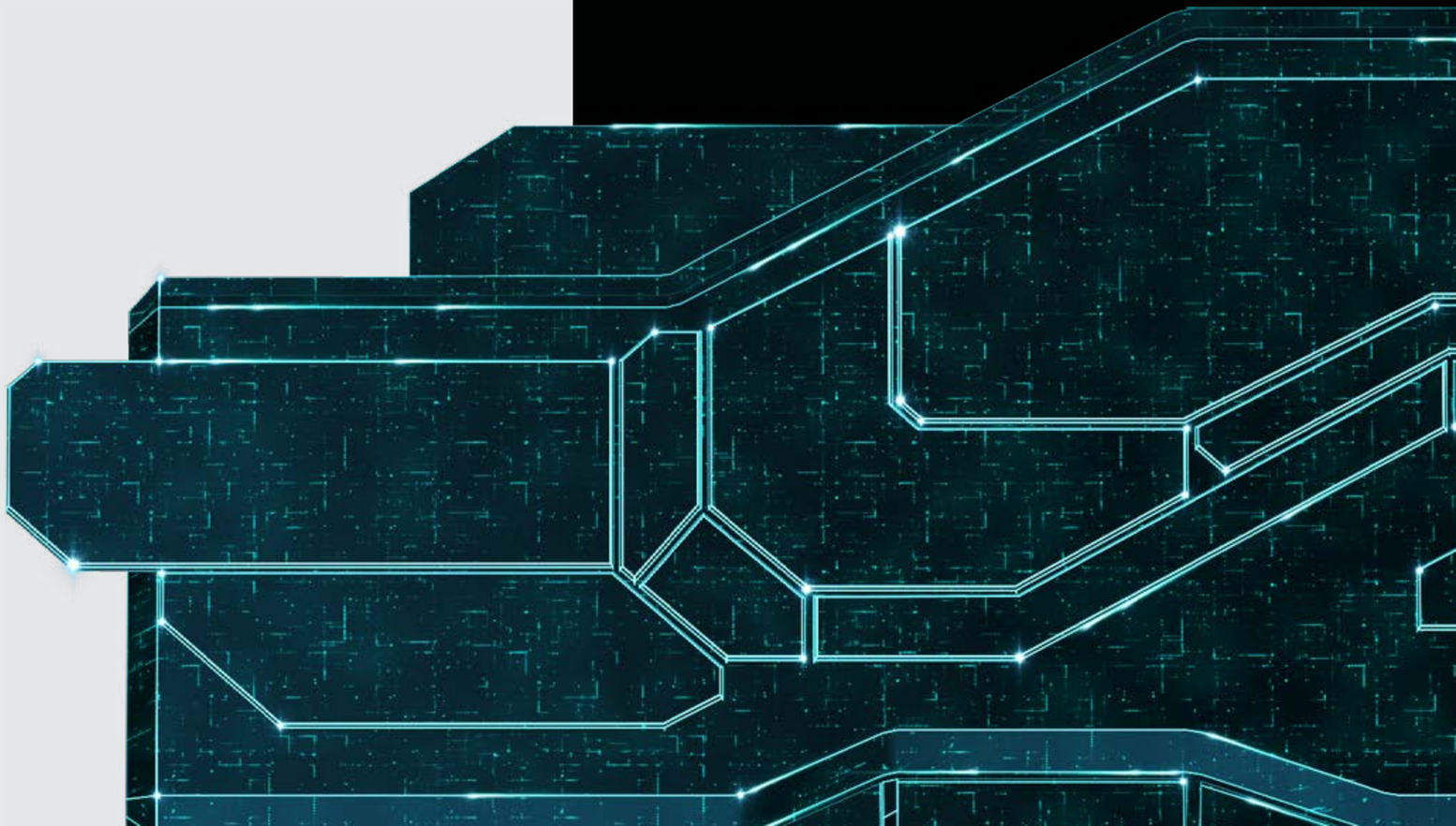
TENDENCIAS DE AMENAZAS WEB BLOQUEADAS POR ESET DESDE EL 4TO TRIMESTRE DE 2019 HASTA EL 1° TRIMESTRE DE 2020, PROMEDIO DE SIETE DÍAS CORRIDOS



PARTE 3

MANTENGA EL RUMBO: 6 CONCLUSIONES PARA EL FUTURO

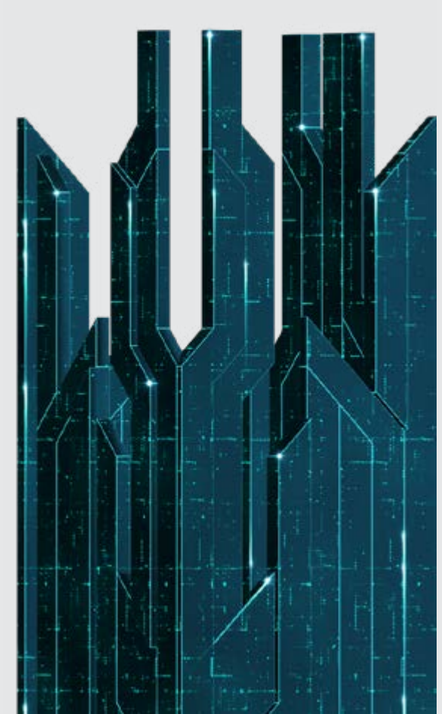
Albert Einstein tenía razón cuando dijo que "*en cada crisis, existe una oportunidad*". La crisis del COVID-19 puede servir como impulsor de una nueva realidad laboral. Los lugares de trabajo digitales y remotos son el futuro, y el futuro comienza ahora. ¿Cómo debemos proceder para gestionar entornos de trabajo seguros y flexibles?



PARTE 3

1. EVALÚE CÓMO LA CRISIS HA AFECTADO SU EMPRESA

Tal vez la crisis finalmente lo llevó a integrar nuevas herramientas y procesos a su rutina y operaciones diarias. Para poder analizar qué soluciones podrían ser útiles en el futuro, primero debe hacerse las siguientes preguntas.



¿QUÉ MEDIDAS MANTENER Y CUÁLES NO DESPUÉS DE LA CRISIS?

- ¿Qué operaciones tuvieron que cancelarse debido a la crisis y por qué?
- En comparación con la situación previa a la crisis, ¿su arquitectura de TI está en mejores condiciones para satisfacer las necesidades comerciales de la empresa?
- ¿La empresa habría resistido mejor la crisis si se hubieran digitalizado más procesos y operaciones?
- ¿Por qué sería favorable o desfavorable para la empresa seguir trabajando en forma remota y buscar una mayor madurez digital?
- ¿Sería conveniente mejorar aún más las políticas y los procesos nuevos que su empresa adoptó durante la crisis?
- De ser así, ¿cuáles son las herramientas y medidas que respaldan esta forma de trabajo y que además serían una buena inversión para el futuro?
- ¿Cómo percibe la gerencia de la empresa las experiencias tanto de la crisis como de la digitalización?
- ¿Cómo perciben sus empleados este modo de trabajo?

PARTE 3

2. REVISE EL ANÁLISIS DEL IMPACTO EN EL NEGOCIO Y EL PLAN DE CONTINUIDAD EMPRESARIAL

Teniendo en cuenta la experiencia de la crisis, junto con el departamento de planificación de continuidad, redefina qué departamentos centrales para el negocio necesitan mejorar su madurez digital.

Ahora debe centrarse en los proyectos que le permitirán trabajar de manera remota. *¿Hay proyectos cruciales para la empresa que hasta ahora no podían transformarse o transferirse al entorno digital? ¿O las soluciones que se le ocurrieron durante la crisis fueron insuficientes?* Es hora de garantizar que su empresa pueda seguir ofreciendo los mismos servicios con la misma calidad pero de modo online.

El análisis del impacto en el negocio y la continuidad empresarial deben reflejar la naturaleza crítica de cada servicio particular, así como el papel que cumple la TI. La crisis puede haber mostrado que algunos planes necesitan revisión: comparta sus conclusiones con los directivos.

¿CÓMO HABLAR CON SU JUNTA DIRECTIVA SOBRE LA SEGURIDAD IT Y EL PRESUPUESTO?

A. DEMUESTRE QUE LA SEGURIDAD IT ES UN ELEMENTO CLAVE PARA LAS NUEVAS OPORTUNIDADES DE NEGOCIO

Las soluciones digitales generan nuevas oportunidades de negocio. No obstante, si la protección de datos es inadecuada, puede dar lugar a enormes pérdidas de información e ingresos, lo que daña la reputación y la confianza general en la empresa. Si les demuestra a los clientes que sus datos están bien protegidos, aumentará la credibilidad de la compañía.

B. PRESENTE SUFICIENTE EVIDENCIA

Muestre estadísticas concretas sobre cómo está aumentando el delito cibernético y cómo un solo clic puede dañar una empresa. Para ilustrar lo peligroso que puede llegar a ser el phishing, por ejemplo, haga una prueba con los empleados de la empresa: envíeles e-mails falsos y vea cuántos hacen clic en el enlace.

Contrate a un hacker de sombrero blanco para que trate de entrar a la red de su empresa.

C. GENERE CONTENIDO PARA APRENDER SOBRE SEGURIDAD IT

Cree materiales de capacitación interactivos para concientizar sobre seguridad IT en la empresa. La gente aprende mucho a través del juego, y la seguridad de los datos no es la excepción.

PARTE 3

3. SI ES NUEVO EN LA DIGITALIZACIÓN, COMIENCE DE A POCO

Si está claro que su empresa aún no ha dado ningún paso significativo hacia la digitalización, no espere poder hacerlo todo en un día. Pero no se preocupe: cada pequeño cambio que implemente es importante. Cree una estrategia de trabajo digital y comience con pequeñas cosas puntuales, como la transición de la contabilidad corporativa a un entorno solamente online. Esto le permitirá administrar sus finanzas desde cualquier lugar y en cualquier momento, y si toda la empresa de repente necesita trabajar en forma remota, la contabilidad digitalizada ya funcionará sin problemas.

En general, encontrar soluciones que ayuden a eliminar el contacto físico entre las personas (cuando sea necesario) es un elemento clave para una digitalización exitosa. Este enfoque también es el apropiado para usar cuando se intenta evitar interrupciones del servicio debido a una enfermedad.

PARTE 3

4. ANALICE SI SUS PROVEEDORES ESTÁN BIEN PREPARADOS

La mayoría de las empresas dependen de proveedores y servicios externos. Si sus proveedores le fallan, es posible que su empresa no resista la crisis. Por lo tanto, es crucial saber qué tan listos están para cumplir con sus obligaciones contractuales o expandir su oferta incluso en tiempos de crisis.

Lo ideal es tener múltiples soluciones para un solo problema. Si falla una aplicación o un servicio, debe haber una solución de respaldo de modo que los empleados siempre puedan realizar sus tareas o comunicarse online.

PREGUNTAS QUE DEBE HACERLES A SUS PROVEEDORES Y SOCIOS COMERCIALES

- ¿Tiene un plan de continuidad empresarial para la pandemia?
- ¿Ha probado su plan de continuidad empresarial en el último año?
- ¿El proceso que suministra a nuestra empresa se vería afectado si un gran porcentaje de sus empleados están ausentes?
- De ser así, ¿aplicó alguna medida para minimizar el riesgo que puede provocar una alta tasa de ausencia entre sus empleados que prestan servicios a nuestra empresa?
- ¿Tiene una lista de proveedores para procesos críticos?
- ¿El proceso que entrega a nuestra empresa puede verse afectado en caso de que sus proveedores interrumpan las operaciones?
- Si es así, ¿ha aplicado alguna medida para minimizar el riesgo que puede causar la interrupción de las actividades de otros proveedores que participan en el servicio que entrega a nuestra empresa?
- ¿Tiene un plan de reanudación de actividades posterior a la crisis?
- ¿Su personal está capacitado en gestión de crisis?

PARTE 3

5. ADAPTE SOLUCIONES DE SEGURIDAD A LOS CAMBIOS

Si bien el cambio a los procesos comerciales online puede mejorar la continuidad del negocio durante la crisis, también presenta riesgos adicionales de seguridad cibernética. Por lo tanto, su obligación no solo es garantizar la buena accesibilidad, sino también proteger los datos corporativos y personales en forma adecuada. Además es imprescindible que las conexiones sean seguras; para ello, es esencial usar una red privada virtual (VPN) de modo de contrarrestar los mayores riesgos de seguridad. Todos los empleados que trabajan en forma remota deben tener una licencia de VPN para poder conectarse de manera segura a la red corporativa.

Otra condición para que el lugar de trabajo remoto y digitalizado sea efectivo es tener suficientes dispositivos que los empleados puedan usar desde su hogar. Pero, *¿qué pasa si su empresa no puede comprar computadoras portátiles o tabletas nuevas justo en este momento?* Entonces considere cuáles son las condiciones para que los empleados usen sus dispositivos personales, como computadoras portátiles, teléfonos inteligentes, equipos de escritorio y tabletas. Como mínimo, cada dispositivo tendrá que estar protegido adecuadamente con una solución antimalware actualizada, que suministre protección para endpoints en varias capas y que sea de un proveedor confiable, no un antivirus gratuito.

PAQUETE BÁSICO DE SEGURIDAD IT PARA UNA DIGITALIZACIÓN EFECTIVA

- Entorno automatizado y estandarizado para una fácil administración remota. Estandarice no solo las herramientas técnicas, sino también los procesos.
- Software de protección para endpoints confiable, que pueda usarse tanto para dispositivos corporativos como personales.
- Cifrado confiable del disco rígido local.
- Monitoreo detallado de cada aplicación y sus datos.
- Uso de contraseñas seguras con autenticación en varias fases y de políticas por grupos efectivas.
- Creación de entornos híbridos combinando implementaciones locales y en la nube para obtener el mejor resultado.

PARTE 3

5. ADAPTE SOLUCIONES DE SEGURIDAD A LOS CAMBIOS

CONSEJOS PARA SUPERAR LOS DESAFÍOS DEL USO DE NUEVAS APLICACIONES.

- Asegúrese de que solo las personas autorizadas estén presentes. Cree grupos de usuarios o restrinja el acceso por dominio de Internet.
- Establezca contraseñas seguras para las reuniones y no las comparta en el mismo enlace de la reunión.
- Pídales a los participantes que aguarden a que se les apruebe la conexión. Cuanto más gente asista a la reunión, mayores serán las posibilidades de que aparezca un participante que no fue invitado.
- Cifre los videos. Tenga en cuenta que algunos servicios solo cifran el chat.
- Establezca un límite de tiempo para intercambiar archivos. No permita que los participantes intercambien archivos ejecutables.
- Elija qué compartir en la pantalla con los demás. Es posible que solo deba compartir una aplicación, no todo el escritorio.
- Revise lo que se ve de su entorno. Incluso los documentos apoyados sobre su escritorio pueden incluir información confidencial.
- Lea la política de privacidad del servicio que está utilizando. Es común que las aplicaciones gratuitas recopilen y vendan sus datos para financiar la prestación del servicio.

CONOZCA MÁS SOBRE CÓMO TENER VIDEO CONFERENCIAS SEGURAS.

MÁS INFORMACIÓN SOBRE CÓMO PROTEGER LOS DISPOSITIVOS DURANTE EL TELETRABAJO.

PARTE 3

6. ACOMPAÑE A SUS COLABORADORES

Aunque para usted la TI es algo común, no todos están tan familiarizados con el mundo digital, por eso debe organizar capacitaciones periódicos de seguridad IT. Además, asegúrese de que los empleados siempre sepan dónde buscar ayuda, una buena solución es tener una casilla de correo para recibir consultas.

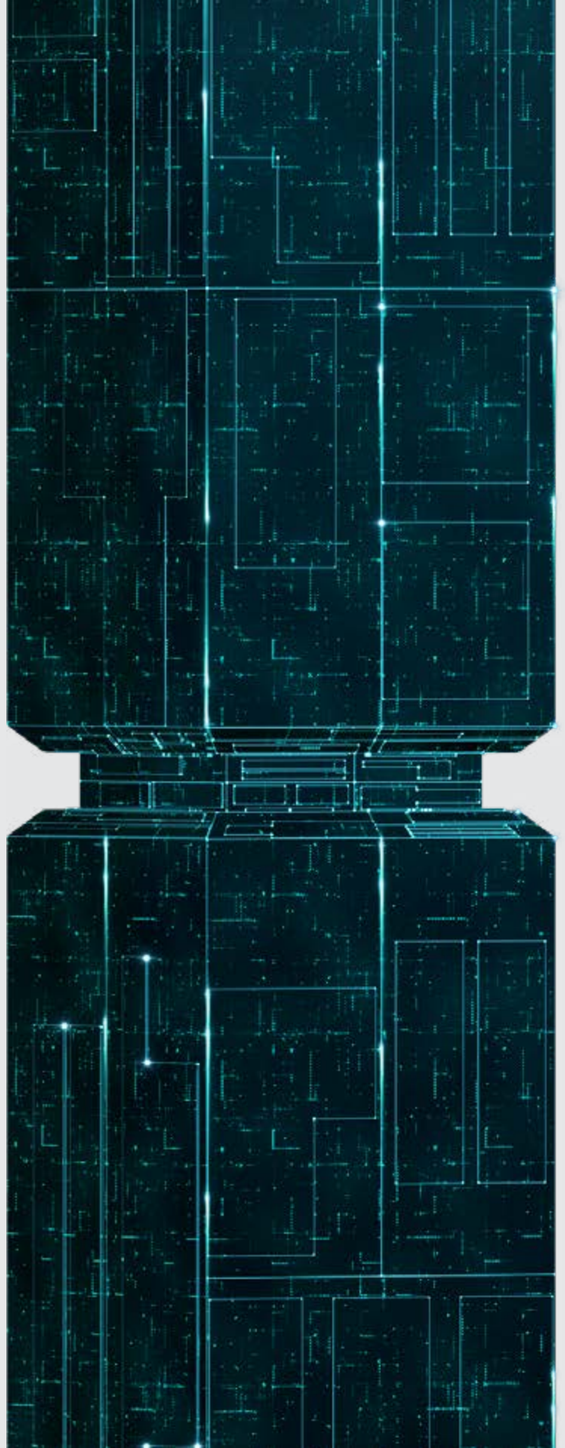
Presente la digitalización y las nuevas herramientas online como componentes útiles, no como una obligación. Las palabras son importantes: hable con claridad y use un lenguaje simple, trabaje en conjunto con su departamento de Recursos Humanos o con los equipos de comunicación. Una corta excursión a la mente humana podría ayudar. Y recuerde que ninguna pregunta es tonta.

Intente evaluar la efectividad de los empleados por tarea, no por hora. El mejor estimulante es la motivación: debe conocer bien a sus empleados y descubrir qué tipo de tareas disfrutan hacer. Las tareas atractivas tendrán los mejores resultados y una alta productividad, y los empleados estarán más abiertos a usar nuevas herramientas digitales. Por último, pero no menos importante, evalúe regularmente los comentarios de los empleados y tenga en consideración sus opiniones, problemas e ideas.

Por otra parte, cuando los empleados están estresados y trabajan de manera remota, es más común que lean y descarguen información de fuentes no confiables. Por ello deben poder diferenciar un e-mail normal de otro de phishing. Una capacitación en alfabetización mediática también puede ahorrarle muchos problemas.

No olvide que el eslabón más débil en la cadena de seguridad es el ser humano. Por eso, debe brindarles instrucciones y capacitación adecuadas para que puedan acceder en forma segura a los sistemas críticos de la empresa desde el entorno doméstico y los dispositivos privados.

Los conocimiento sobre malware, virus y phishing, ayudan a prevenir el manejo de las amenazas actuales, que de lo contrario podrían poner en riesgo a la empresa.



PARTE 3

6. ACOMPAÑE A SUS COLABORADORES

Le recomendamos que comparta los siguientes consejos de seguridad con ellos.

¿CÓMO ENCONTRAR FUENTES SOSPECHOSAS DE INFORMACIÓN?

- Falta la fecha de publicación.
- Falta el autor del artículo.
- La conexión no es segura (falta el ícono del candado en el campo URL).
- En el contenido aparecen muchos signos de exclamación.
- Se requiere una acción inmediata; por ejemplo, compartir datos.
- El contenido está repleto de errores gramaticales.
- El contenido es gráfico.
- Aparecen frases como "*Por qué los medios no hablan de esto*".

¿CÓMO NO CAER EN UNA ESTAFA DE PHISHING?

- Evalúe lo que le están pidiendo. ¿La solicitud sospechosa?
- Si el remitente usa el nombre de un empleado de la empresa, comuníquese con él a través de un canal confiable, o escríbale un e-mail nuevo e inserte la dirección del remitente. Pregúntele si realmente lo contactó.
- No acepte archivos y no haga clic sobre cualquier cosa que aparezca en e-mails de desconocidos.
- Antes de hacer clic en un vínculo a un sitio web, búsquelo en Google. Si el nombre del remitente es familiar, búsquelo también.
- Revise si hay errores gramaticales.
- No envíe ninguna información confidencial por e-mail.
- De ser posible, informe si recibió un e-mail.

MÁS INFORMACIÓN SOBRE CÓMO NUESTRAS SOLUCIONES BLOQUEAN EL PHISHING.

CONCLUSIÓN:

NO HABRÁ BUENOS NEGOCIOS SIN UNA BUENA TI

Aquí le explicamos por qué las empresas deberían centrarse (hoy) en la digitalización y en tener una excelente infraestructura de TI.

AUMENTARÁN LAS AMENAZAS CIBERNÉTICAS

La cantidad de dispositivos que operan online se está incrementando con rapidez, y los ciberdelincuentes perfeccionan sus tácticas e implementan inteligencia artificial sofisticada para mejorar la propagación y eficacia de su malware. Atrás quedaron los tiempos en que los correos electrónicos de phishing eran muy fáciles de detectar.

El informe de preparación en ciberseguridad Cybersecurity Readiness Report 2019, publicado por Hiscox, que encuestó a alrededor de 5.400 profesionales de los Estados Unidos, el Reino Unido, Alemania, Bélgica, Francia, España y Holanda, declaró que alrededor del 61% de las empresas experimentaron un ataque cibernético en 2019, en comparación con el 48% en 2018. *"A nivel mundial, el costo promedio de la pérdida asociada con un incidente cibernético ha aumentado de USD 229.000 a USD 369.000"*, indica el informe.

LA FLEXIBILIDAD ATRAERÁ LOS TALENTOS

Cada vez son más las personas que piden flexibilidad en el trabajo, lo que se puede lograr si se integran soluciones y herramientas online que les permitan a los empleados trabajar de manera remota. Un lugar de trabajo digitalizado no solo facilita mantenerse seguros y productivos en tiempos de crisis, sino que también ayuda a atraer más talentos, principalmente a los *millennials* (nacidos en las décadas de 1980 y 1990), y a la Generación Z (nacida entre fines de la década de 1990 y 2010), que recién está ingresando al mercado laboral. Un estudio llevado a cabo en 2018 por el Pew Research Center demostró que en 2016 los *millennials* se convirtieron en la generación más grande de la fuerza laboral estadounidense y, por lo tanto, es crucial satisfacer sus necesidades, que entre otras incluyen la flexibilidad horaria en el trabajo.

Otra investigación realizada por *PwC* señaló que no son solo los *millennials* sino todas las generaciones de trabajadores quienes buscan empleos más flexibles y que ocasionalmente les permitan trabajar desde casa. *"Las similitudes de la actitud entre distintas generaciones son sorprendentes"*, afirma el estudio. Por eso, cuando se implementan soluciones flexibles y digitalizadas, los empleados de todas las edades pueden estar más satisfechos, motivados y ser más productivos.

CONCLUSIÓN:
NO HABRÁ BUENOS NEGOCIOS SIN UNA BUENA TI

MANTENGA SU EMPRESA A PRUEBA DE CRISIS

La situación a raíz del COVID-19, demostró que las empresas que lograron digitalizar sus procesos y activos resistieron la crisis mucho mejor que las que no lo hicieron. Expertos coinciden en que nos esperan más situaciones como estas,por lo tanto, el teletrabajo y los entornos digitalizados y bien protegidos, no solo serán una ventaja competitiva, sino también una necesidad.

Como consecuencia, las empresas deben darse cuenta de que la TI es su mejor socio de negocios y que, en el futuro, no podrán operar sin profesionales de TI calificados ni soluciones avanzadas de seguridad TI. La crisis de COVID-19 puede ser un punto de inflexión gracias al cual la sociedad finalmente comience a percibir la digitalización de manera más positiva.

CONTÁCTENOS PARA SABER MÁS SOBRE NUESTRA EXPERIENCIA O PARA SOLICITAR AYUDA CON LA SEGURIDAD DE SU ENTORNO REMOTO.