BOLETÍN INFORMATIVO núm.2 **Precauciones en el nuevo escenario de trabajo**	**Nuevo escenario de trabajo por el COVID-19** 
• **Las WIFIs** • **El correo** • **Bulos y desinformación** • **Las videoconferencias y el trabajo colaborativo**	En el primer boletín de seguridad realizado durante este periodo de confinamiento repasamos las mejores prácticas y conocimos los riesgos que nos acechan cuando debemos usar el teletrabajo para desempeñar lo que son nuestras actividades laborales en un nuevo entorno des-localizado. Es usual que se acabe acusando a los técnicos en seguridad de ser excesivamente reiterativos en los mensajes que damos, pero es que, basándonos en nuestra experiencia, observamos que los errores comunes que facilitan la entrada de ataques son, en realidad, fácilmente corregibles cuando los usuarios están formados y concienciados. A lo largo de los últimos años, el Servicio de Seguridad de la Administración del Principado de Asturias (APA) ha estado redactando boletines trimestrales que trataban, de forma sencilla, la mayor parte de cuestiones que tienen que ver con la mejor forma de comportarse para proteger nuestros datos y equipos; esos boletines, que pueden consultarse en la Intranet de la APA **(https://intranet.asturias.es, canal Para ti – Para tu trabajo – Seguridad de la Información**) incluían recomendaciones -uso adecuado de contraseñas, realización de copias, precauciones en el uso de redes WIFI, vigilancia ante las acciones de los hackers contra los correos, manejo de contraseñas robustas, prácticas delictivas habituales, entre otras muchas- que son plenamente válidas en el actual escenario de “alarma”, pero es verdad que ahora hay, incluso, que extremar esas precauciones dado que el teletrabajo se materializa a través de mecanismos cuya capacidad de defensa es inferior a la que habitualmente disfrutamos en los equipos y redes corporativas. Dado que ya en el boletín de hace unas semanas introducíamos los conceptos básicos de la seguridad en este entorno de trabajo en remoto, vamos ahora a insistir y profundizar en algunas de esas cuestiones, basándonos también en las numerosas preguntas o dudas que otros compañeros nos han ido trasladando estos días (y que ilustran bien la cada vez mayor preocupación de los trabajadores por estos temas).

Las WIFIs

En vez de estar trabajando desde un PC corporativo en la oficina, ahora debemos trabajar desde nuestros propios equipos personales en casa, y tirando de la propia conexión a Internet de nuestro hogar. Por tanto, esos dos puntos son críticos, ni el ordenador de casa ni la conexión del router, sea directa o por WIFI, han sido securizados bajo los estándares de la Administración.

Desde luego, el primer error sería usar en el teletrabajo una conexión ajena, por ejemplo una WIFI pública y gratuita, dado que lo que hacemos en una de esas redes abiertas es muy sencillo de capturar por parte de un hacker. Pero incluso siendo nuestra conexión hay que pensar que tanto el router como el "camino" del PC a ese router a través de un medio inalámbrico son activos poco robustos, y tampoco tiene por qué serlo el camino entre ese router e Internet. Entre las prácticas favoritas de estos individuos (y aprovechamos para ir comentando términos relativamente técnicos) están el "**man in the middle**", donde el hacker consigue que la comunicación entre el router e Internet pase a través de un equipo pirata que observa todo el tráfico de datos y captura lo que le interesa. En ocasiones esta captura de la información se hace directamente suplantando nuestro router con lo que se llama "**rogue AP**" y permitiéndonos salir a Internet no vía , sino a través de otro que está bajo control de los atacantes.

Intentar evitar estas debilidades pasa por fortalecer el router, pero ello es algo que habitualmente no hacemos, salvo en lo que es cambiar el nombre con el que vienen de fábrica; en cambio, pocas veces modificamos la contraseña del router (con el peligro de que esas credenciales se suelen encontrar en diccionarios que los hackers poseen).
Las recomendaciones habituales (pero reconocemos que muchos usuarios pueden tener dudas sobre su forma de cumplirlas) implican entrar en el router (siguiendo la instrucción que cada modelo aplica) y realizar cosas como:

- Cambiar la contraseña de fábrica del dispositivo y sustituirla por una de grado fuerte (que incluya, al menos, 8 caracteres y entre ellos dígitos, caracteres especiales y letras minúsculas y mayúsculas).
- Deshabilitar el WPS (Wifi Protected Setup) para impedir que se use la red sin haber introducido una contraseña previamente.
- Revisar que se usa un protocolo de red seguro (del tipo de WPA2 o, mejor, el WPA3).

El correo

Muchos compañeros y compañeras nos han preguntado estos días por qué el correo es siempre tan mentado al hablar de protección. La respuesta es sencilla, el correo es lo que llamamos vector de entrada fundamental de ataques; el malware no entra tan a menudo a través de páginas WEB como de correos. Estos emails intentan engañar haciéndose pasar por correos "inocentes", o remitidos por conocidos, organismos oficiales o entidades comerciales y bancarias. El asunto que incluyen trata de atraer la atención incluyendo textos como "último aviso", "cobro", "facturas" o, en estos momentos de pandemia, palabras del tipo "COVID19", "cura del coronavirus", "medidas contra el virus". **El último caso de PHISHING activo detectado es el que se hace pasar por un envío de la Inspección de Trabajo y Seguridad Social, y que aunque ya hemos bloqueado en nuestra Administración, seguirá buscando camuflarse y engañar a los usuarios.**

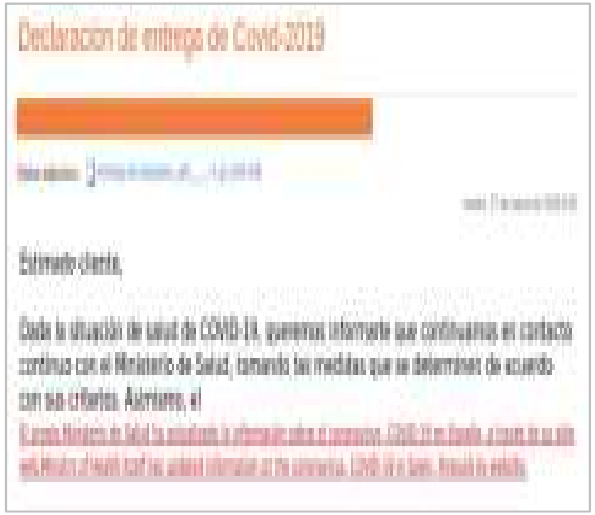
Los correos maliciosos pueden llegar por miles y muchos de ellos son de calidad, en cuanto a su capacidad de convicción o engaño; por tanto, la mejor medida contra ellos es la permanente desconfianza contra todo correo sospechoso.

Sabemos que no es sencillo a veces distinguir un PHISHING (correo con engaño) de uno real, pero es

necesario intentar seguir siempre estas prácticas:

- Se ha de revisar bien el nombre del remitente y su dominio (la parte que va detrás de la @); si no le suena o es un remitente habitual conocido o parece de procedencia extranjera, lo mejor que puede hacer es evitar abrirlo. Incluso puede ser aconsejable mandar un correo a esa dirección para preguntar sobre la identidad real del que lo ha enviado.
- Si el correo solicita introducir datos personales, datos bancarios o contraseñas, se trata de un ataque.
- Si el correo es de un destinatario desconocido o sospechoso y anima a pulsar enlaces o abrir adjunto, se ha de ser especialmente cauto.
- Si el correo o un adjunto abierto anima a acciones tales como "habilitar las macros de las Office" o a "habilitar la pre-visualización automática de correos" no realice ninguna actividad, se ha de informar a los responsables de seguridad.
- Si el correo dice estar remitido por una entidad financiera, un organismo oficial, una empresa de venta por Internet, un proveedor de Internet, sea igualmente cauteloso y no muerda el cebo; si se solicita introducir datos bancarios o credenciales de usuario , estará, con casi total seguridad, ente un engaño.

Algunos ejemplos de PHISHING que estos días han intentado difundirse por nuestros correos de la APA::



Bulos y desinformación

Mientras que los correos y páginas fraudulentas suelen perseguir dinero, bien sea secuestrando los equipos y pidiendo un rescate, o bien robando datos de cuentas bancarias o tarjetas de crédito, existe otro tipo de ataques que generalmente están encuadrados en lo que se conoce como campañas de desinformación. Su herramienta de difusión es el correo electrónico, los mensajes de WhatsApp o los comentarios en redes sociales.

Sean lanzadas por individuos aislados o sectores partidistas nacionales, o sean movidas por hilos internacionales, el efecto final es el de contribuir a la alarma social, a la pérdida de cohesión y confianza entre la población y sus instituciones o al incremento de ideologías extremistas y reaccionarias.

En este caso las normas comunes de comportamiento inciden en:

- No difundir ni reenviar masivamente mensajes que no provengan de fuentes oficiales o fiables (y precaución aquí dado que en algunos casos los "trolls" pretenderán hacer pasar sus mensajes como emitidos por entidades públicas o acreditadas).
- Si detecta un ataque a personas (bien individuales o como integrantes de grupos significados ideológica, étnica o religiosamente) no contribuya a la extensión de una campaña de odio.

Recuerde siempre que en muchos casos es un posible delito el envío de determinados mensajes y videos en las redes sociales.

- No se ha de ayudar a desinformar repartiendo mensajes catastrofistas o que prometen curas milagrosas; especialmente en la situación actual, su difusión en poco ayuda a contener la epidemia o la alarma social

- Antes de remitir determinado mensajes en correos, mensajerías o redes sociales, se ha de invertir trabajo de buscar mínimamente en Internet sobre la posible fiabilidad del contenido. Son útiles a veces las páginas que se dedican a desmontar este tipo de bulos, entre ellas:
  https://maldita.es
  https://www.vost.es/stopbulos

Las videoconferencias y el trabajo colaborativo

Entre las herramientas más usadas en época de teletrabajo están las vídeocomunicaciones en grupo, que facilitan el desarrollo de lo que serían reuniones en remoto. Su crecimiento está siendo exponencial y, así por ejemplo, ZOOM ha pasado en tres meses de tener 10 millones de usuarios a más de 200 millones.

Hay una serie de precauciones lógicas a recordar, la primera es que no todas las herramientas para trabajo colaborativo, que suelen incluir sistemas de "vídeo reuniones", cumplen unos mínimos niveles de seguridad y protección, ni garantizan que los datos que se generan en dichos sistemas no sean difundidos o reutilizados irregularmente.

Es verdad que se trata de plataformas que no eran usadas habitualmente y el hecho de ignorar el funcionamiento óptimo de las mismas puede llevarnos a confusiones (envío de mensajes privados a quien no se pretende, publicaciones en grupo que no se pretendían hacer, compartición de la pantalla del ordenador poniéndola a la vista de otros usuarios, etcétera).

En todo caso apuntemos como aspectos "formales" a recordar, el hecho de que cuando se participa en una videoconferencia todos le pueden ver o escuchar en la intimidad de su hogar y rodeado de su familia, así que ha de aprender pronto a manejar el micrófono, la cámara y las formas de desactivarlas. Sea cauto también con la mensajería pues no son pocos los usuarios que intentando mandar un mensaje a un participante lo lanza a todos los asistentes.

Incidimos luego en el hecho de que lo que se dice en vídeo puede grabarse o difundirse pero contando con permisos de los participantes, dado que existen una serie de derechos sobre la imagen y los comentarios de los intervinientes que han de respetarse.

Trabajar en remoto, desde el hogar, y sirviéndose de plataformas colaborativas, no puede ser motivo para que ignoremos las regulaciones sobre protección de datos personales y las obligaciones de impedir que los datos de la organización pululen sin control por redes abiertas o en almacenamientos en la nube de escasa credibilidad.
Un debate bien habitual estos días es el que tiene que ver con la seguridad, o falta de ella en algunas de esas herramientas; ello es suficiente motivo como para tratar de evitar el "ir por libre" y seguir las instrucciones o recomendaciones que la organización haya dado al respecto; indiquemos ahora algunas de estas vulnerabilidades, aunque no olvidemos, tampoco, que las propias compañías fabricantes han intentado parchear de manera inmediata sus productos para minimizar esos puntos débiles:

- Fugas de datos hacia otras aplicaciones y redes, como Facebook.

- Debilidades en el sistema de encriptado de los datos que se mueven en la reunión (lo que podría facilitar su robo por parte de hackers o usos no aclarados por parte de las propias compañías).
- Difusiones entre los usuarios de las aplicaciones de videoconferencias de cientos de cuentas de otros usuarios, sin permiso de éstos.
- Introducción ilegítima de enlaces maliciosos que ese mueven por los chats de las aplicaciones de videoconferencia, en lo que los usuarios pinchan, facilitando entonces y sin ser conscientes de ello, el ataque de los hackers.

En general las compañías propietarias están intentando ajustar sobre la marcha sus herramientas y sus políticas de uso y privacidad de datos, y, por ello, puede ser conveniente, en caso de necesitar usarlas, el ir actualizando a las más nuevas versiones de esas herramientas.

Hay especialistas que recomiendan evitar las aplicaciones de videoconferencias más "de moda" para acudir a otras herramientas gratuitas y menos extendidas que suelen ser de código abierto, que no obligan a instalar nada en los equipos y que parece que han presentado más robustez, sin ser ello algo que nosotros podamos afirmar o garantizar.

En un escenario de teletrabajo la posibilidad de que los servicios informáticos de la Administración podamos bloquear aplicaciones en uso, es reducida, y sabemos que los usuarios pueden tener facilidad para operar con herramientas que no son las que se están recomendando para ejercer el teletrabajo cooperativo. No es una práctica adecuada. **La aplicación que se considera en estos momentos como "corporativa" sería el office 365 y su sección de trabajo para grupos, Teams.**

Otra herramienta que puede haber usuarios que estén manejando es, precisamente, Zoom, que ha sido estos días objeto de enconadas críticas por sus deficiencias en seguridad; no obstante creemos justo exponer la conclusión del Centro Criptológico Nacional (CCN) que entiende que salvo para sectores que manejen información sensible las versiones últimas han subsanado deficiencias y pueden ser usadas.

Para aquellos interesados en conocer más al respecto, se aconseja consultar la información de CCN: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/9911-como-utilizar-la-plataforma-zoom-de-forma-segura-2.html

También el CCN ha elaborado interesante documentación referida al uso del Teams y a sus configuraciones avanzadas, pero, en cualquier caso, debe resaltarse el hecho de que esta plataforma de Microsoft fue diseñada aplicando criterios de seguridad para potenciar su robustez ante ataques y un uso correcto de los datos que maneja. Ante dudas sobre el manejo de Teams puede acudir a los medios que la organización ha puesto para informar sobre el mejor uso de la herramienta así como atender posibles incidencias que les surjan.

COMO RESUMEN FINAL, RECUERDE, POR FAVOR, QUE:

-UN TELETRABAJO SEGURO DEPENDE EN GRAN MEDIDA DEL USUARIO/A Y SU CONOCIMIENTO DE LOS RIESGOS QUE EXISTEN.

-HAY CAMPAÑAS ACTIVAS DE HACKERS CONTRA EMRESAS Y ADMINISTRACIONES PARA INFECTAR EQUIPOS Y ROBAR DATOS Y CONTRASEÑAS. NOSOTROS NO SOMOS UNA EXCEPCIÓN.

-SEA ESPECIALMENTE CAUTO CON LOS CORREOS QUE RECIBE. PUEDEN SER PHISHING, CORREOS FALSOS QIUE TRATARÁN DE QUE DESCARGUE ARCHIVOS O ENLACES INFECTADOS O QUE ENTREGUE CREDENCIALES Y REALICE PAGOS.

-LOS SERVICIOS DE SEGURIDAD INFORMÁTICA DE NUESTRA ADMINISTRACIÓN SIGUEN ACTIVOS Y, COMO MUESTRA, HAN BLOQUEADO DESDE EL INICIO DE LA CRISIS MILES DE DOMINIOS DE INTERNET FRAUDULENTOS, MÁS DE 30.000 CORREOS SPAM, Y 130.000 AMENAZAS DETECTADAS POR NUESTROS FIREWALLS.