Introducción

El medio de trabajo digital es cada vez más prevalente y seguirá en alza en los años venideros. Por ello es tan importante no solo saber cómo funcionan las nuevas tecnologías aplicadas al trabajo, sino también como protegernos de acciones maliciosas que nos pueden llegar por estos medios.

Podríamos decir que navegar por internet es como andar por la calle: hay zonas relativamente seguras y otras que no y adoptamos una mentalidad de seguridad personal y sentido común dependiendo de donde estemos. El problema es la abstracción de internet y del ordenador. ¿Qué me podría pasar desde la comodidad de mi casa u oficina? Llevamos una vida entera utilizando pantallas, principalmente para nuestro entretenimiento y jamás nos han hecho daño. Esta es la mentalidad con la que los hackers están contentos de que tengamos. Quieren que tengamos la guardia baja.

Cada día es más fácil aprender a explotar vulnerabilidades en ordenadores y servicios online. Existen grandes grupos organizados dedicados exclusivamente a la ciberdelincuencia, muchos de ellos provenientes de China o Rusia (grupo Killnet por ejemplo) pero hasta menores pueden aprender estas habilidades desafiando a grandes empresas como Rockstar Games y Uber o incluso administraciones públicas como la Policía o la DGT.

Por ello es tan esencial aprender a protegernos con una serie de habilidades mínimas que nos pueden ahorrar un disgusto. Con esta serie de consejos, ya estamos a un paso más adelantado que la mayoría de la gente y podremos evitar ataques o estafas comunes.

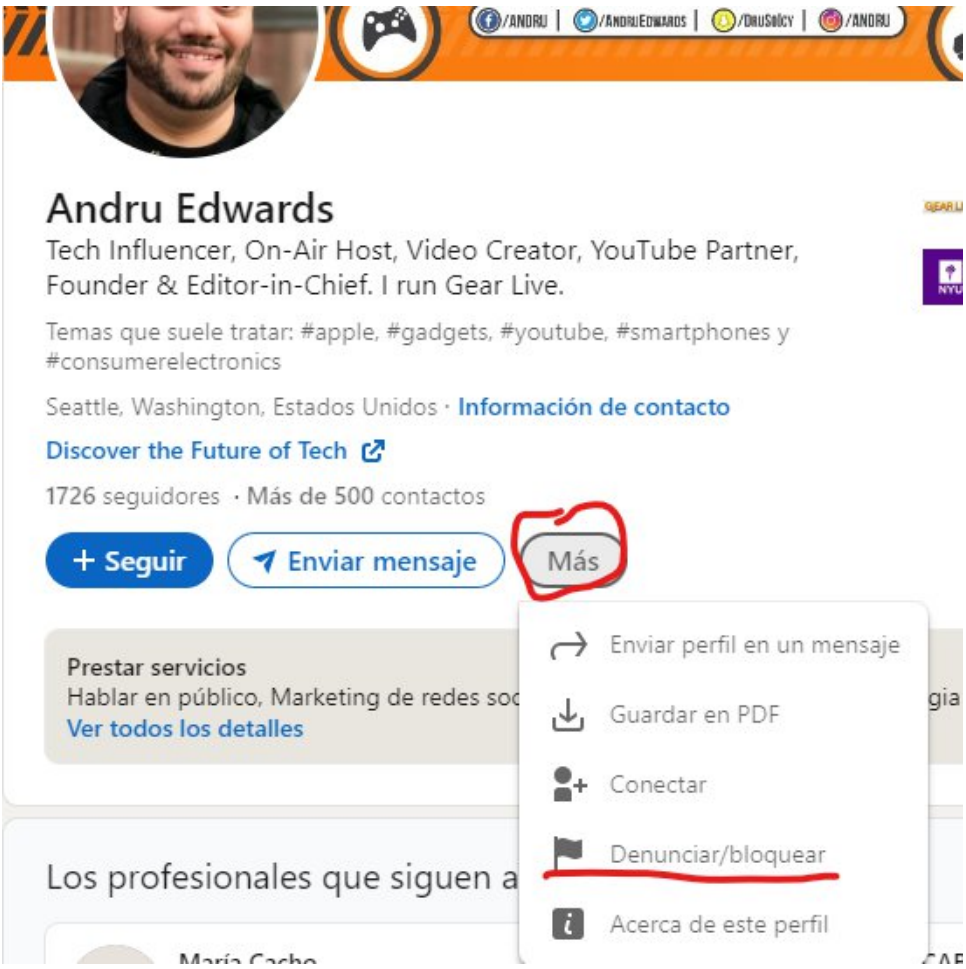
Seguridad en redes sociales

En redes sociales, no aceptar contactos sin mirar antes su legitimidad. Podemos mirar antes la actividad de la cuenta, cuánto tiempo lleva la cuenta creada, qué conexiones tiene, etc...

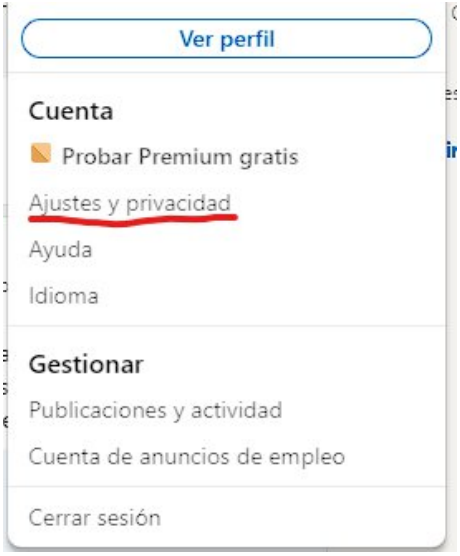
Entra en el perfil y mira si sus publicaciones son consistentes y si están bien escritas.

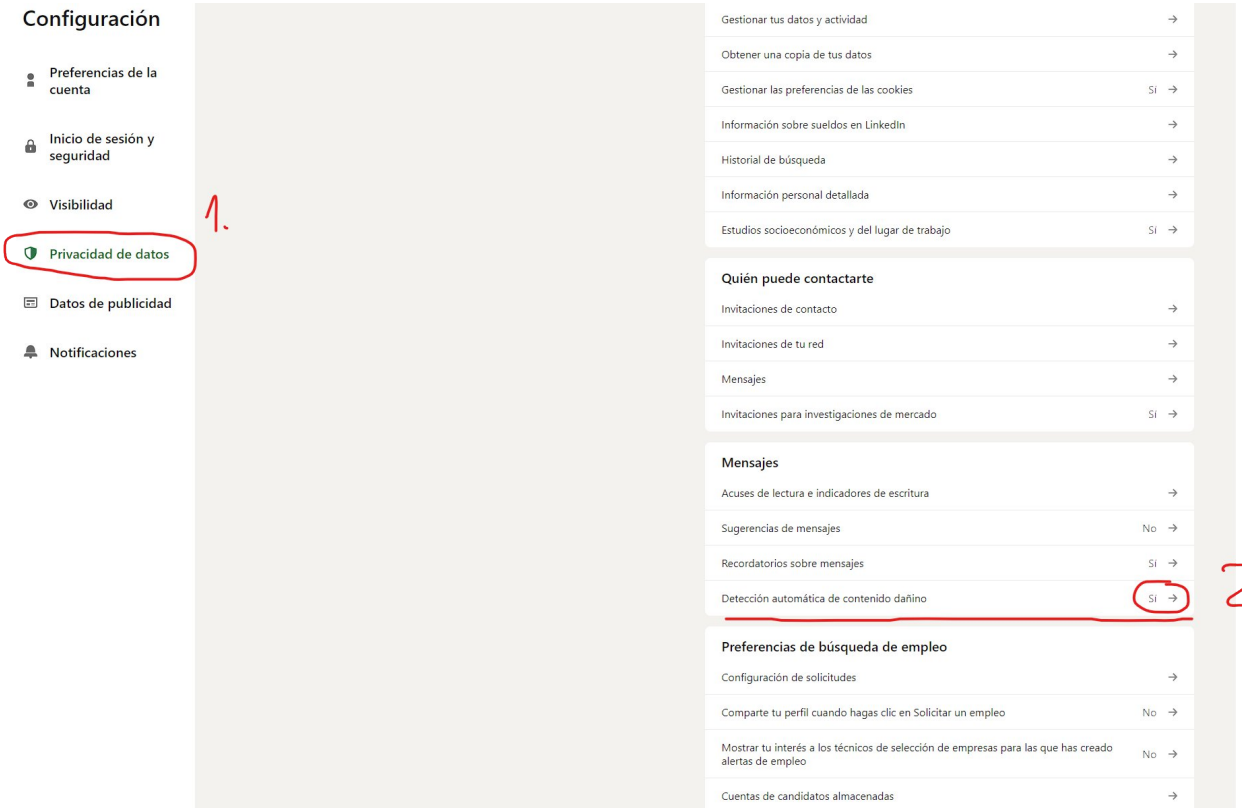
Si no nos inspira confianza, podemos simplemente rechazar la invitación, especialmente si ha venido sin mensaje que explique quien es.

Si la cuenta no solo no inspira confianza sino que la invitación también viene acompañada de reclamos falsos, o peticiones o promesas de algún tipo, podremos reportar o denunciar la cuenta para que Linkedin investigue. Si tuviera una página web, podemos comprobar cuánto tiempo lleva operativa y en qué país se ha registrado en la siguiente dirección: [WHOIS | Lookup Domains and Check Availability - Domain.com]



Algunas redes también tienen detección de archivos potencialmente maliciosos. Es decir, si alguien te contacta por chat enviando un archivo, Linkedin puede detectar si el archivo puede ser un peligro. De todas formas, como sentido común, no aceptes archivos de extraños, aunque Linkedin o la red social no te avise de que sea peligroso. Para habilitar esta función en Linkedin, pulsa sobre “Yo” y luego en “ajustes y privacidad”. Aquí, dentro de “privacidad de datos” activa “Detección automática de contenido dañino”





En correos electrónicos y números de teléfono

Conviene separar correos profesionales de los privados para tener claro la proveniencia. Con un cliente de correo en PC como Outlook o Thunderbird, se pueden separar ambas bandejas de entrada. Incluso en aplicaciones móviles. Aún así, se recomienda separar ambos ámbitos en dispositivos distintos. Es decir, un ordenador o móvil para el trabajo solamente.

La gestión de los correos (es decir, su eliminación o clasificación en carpetas) es mejor llevarla a cabo en un PC porque permite ver más información sobre el correo en cuestión de una manera más calmada. Correos sospechosos con direcciones extrañas o asuntos extraños no deben ser abiertos.

Aún en el caso de abrir algún correo sospechoso de manera accidental, muchos servicios de correo implementan una protección que pide permiso para cargar imágenes externas al correo y nos protege de vulnerabilidades. Esto es así porque las imágenes son cargadas desde una página web externa, no vienen incrustadas dentro del correo electrónico. Al permitir la carga de imágenes de un correo potencialmente malicioso, estamos dejando vía libre de acceso a nuestro dispositivo.

En muchos casos hay que aceptar que correos y números corporativos son objetivos principales de ataques (piensa correos o números que están públicamente en el mundo: en anuncios, páginas web oficiales, los que compartimos con cientos de clientes, etc...) y es inevitable que haya intentos de vulneración. Por eso se recomienda que estos datos públicos jamás se usen para acceder a cuentas que necesiten más seguridad. Es decir, si usamos un correo electrónico que está públicamente en nuestra web y se usa para contestar a cientos de clientes, no la usaríamos para acceder a nuestras bases de datos. Es recomendable crear una dirección de correo electrónico distinta para este tipo de accesos y que jamás se revele al público. Podemos monitorizar si nuestra dirección de correo electrónico y número de teléfono se ha compartido en foros de hackers o en listados de potenciales ataques usando la página web [Have I Been Pwned: Check if your email has been compromised in a data breach]

Puedes probar a meter los datos de un correo público (que lo más seguro es que te aparezca como una vulnerabilidad) y luego otra cuenta de correo menos expuesta y comparar. Hay que recalcar que en el momento un correo o número de teléfono aparezca en estas listas, no existe solución para ello. En el caso de correos públicos, como bien se ha dicho al principio, hay que aceptarlo y aplicar medidas de sentido común y seguridad pero con correos que supuestamente deberían ser más privados o se usen para acceder a servicios críticos, lo mejor es crear otra cuenta de correo para ese fin y determinar cómo se ha llegado a exponer el antiguo para no repetirlo.

Activar autenticación de dos pasos dónde esté disponible

La autenticación de dos pasos es un método de seguridad que se debe activar en todos los servicios que podamos. Tradicionalmente, el acceso a una cuenta se realiza con un usuario y una contraseña. Sin embargo, en el caso de que estos dos elementos son conocidos por un atacante, sería muy fácil que nos entrasen a la cuenta.

Con la autenticación de dos pasos no solo no basta con poner una contraseña, sino que también deberemos autorizar la entrada con una aplicación en nuestro móvil así asegurándonos de que las entradas a la cuenta estén controladas.

Aplicaciones recomendadas son Microsoft Authenticator o Authy. Ambos tienen función de guardado de las claves de autenticación de forma encriptada en la nube de estas compañías así que en caso de pérdida o robo del móvil, se puede recuperar las claves en un dispositivo nuevo y desvincular el dispositivo vulnerado. Si nunca se ha usado una aplicación de autenticación, hay que saber que no basta con descargar e instalación la aplicación en el móvil. Hay que activar el método de seguridad en la cuenta de ese servicio, normalmente localizado en los ajustes de la página web. En Linkedin se encuentra un artículo de cómo activarlo en algunas páginas web populares:

Como activar el factor de doble autenticación o MFA | LinkedIn

En casos extremos, se puede usar un Yubikey pero todo depende del perfil de riesgo que tengas. Yubikey es el mismo concepto de autenticación, pero ya por uso de un medio físico en forma de llave USB. Cada vez que tengamos que autorizar un acceso a una cuenta, en vez de hacerlo con una clave generada en una aplicación, tendremos que físicamente enchufar el Yubikey en el dispositivo. Es más inconveniente pero mucho más seguro. En el caso de comprar un dispositivo de seguridad de este estilo, se recomienda que jamás los compres de un distribuidor o tienda de terceros como Amazon y muchísimo menos de segunda mano. Puede haber un riesgo de que alguien lo haya manipulado previamente. Es mejor comprarlo desde la página oficial de la compañía:

La YubiKey - Yubico

Vídeos relacionados:

¿Qué es la verificación en dos pasos?

Creación de contraseñas debe ser tan aleatoria como sea posible.

Lo ideal es siempre tener una contraseña distinta para cada servicio, de al menos 12 caracteres y mezclando letras mayúsculas, minúsculas, números y símbolos. El problema es que es imposible para una persona memorizar este tipo de contraseñas, especialmente si usa muchos servicios.

La herramienta que usan muchas personas preocupadas por este aspecto es algo llamado gestores de contraseñas. Son un servicio que genera y guarda contraseñas complejas y te las aplica automáticamente cuando detecta que necesitas iniciar sesión en un servicio. Lo único que pide para su uso es que uses una contraseña maestra que tengas memorizada y no hayas usado en ningún otro lugar para acceder al gestor. Con esto, tan sólo hace falta memorizar una sola contraseña para acceder al resto. Por encima, aunque alguien quisiera hackear estos servicios, las contraseñas están encriptadas y sin esa contraseña maestra, no se pueden leer. La más popular es Bitwarden que tiene tanto extensión de navegador como aplicación móvil y es totalmente gratuita al ser un programa de código abierto, está hecho por el amor al arte y es seguro ya que se puede auditar que el programa no hace nada raro con tus contraseñas.

Cabe mencionar que hoy en día, los navegadores web como Chrome, Opera, Safari o Firefox también tienen su versión de gestor de contraseñas (cada vez que te preguntan de guardar la contraseña en alguna página web) y suelen almacenar las contraseñas dentro de sus ajustes. El problema es que los navegadores no encriptan las contraseñas como lo hace un gestor decente entonces en caso de hackeo, cualquiera puede leer las contraseñas.

Aún así, si no quisieras pasar por usar un gestor de contraseñas dedicado, lo mínimo es generar contraseñas aleatorias usando el navegador y dejando que las recuerde por ti. Si usas la misma cuenta del navegador, incluso puede sincronizar las contraseñas con tus otros ordenadores y móviles haciendo que nunca debas recordar otra contraseña.

Por último, subrayar que dejar que el navegador guarde las contraseñas puede ser un peligro si compartes la cuenta del navegador como ocurre aquí en Milcom para ciertas cuentas (aulavirtualmilcom por ejemplo). El mayor culpable es Google. Si iniciamos sesión en nuestra cuenta de Google o Gmail, el navegador Chrome también lo hará, haciendo que si visitas páginas más personales como Amazon o cuentas bancarias, las contraseñas queden guardadas en esa cuenta de Google compartida y los podrá ver las otras personas con las que compartas la cuenta.

Conviene siempre acceder a https://myaccount.google.com/security no solo en cuentas compartidas sino también en las personales para revisar el estado de seguridad de nuestra cuenta. Desde aquí podemos revisar qué contraseñas tiene guardadas Google, qué dispositivos han iniciado sesión en nuestra cuenta y la posibilidad de activar autenticación de dos pasos.

Vídeos relacionados:

Bitwarden - Gestor de contraseñas

Cómo proteger mi cuenta de Google