Unidad 3. Seguridad y Privacidad

Uno de los aspectos que debemos cuidar cuando trabajamos con el correo electrónico es la seguridad y privacidad. En los últimos años se han implementado varios mecanismos para lograr aumentar la seguridad de nuestras cuentas de correo, pero no cabe duda que la herramienta más eficaz es una buena gestión del mismo por parte de los usuarios. En este apartado vamos a ofrecer algunos consejos prácticos para minimizar el riesgo de que nuestra cuenta sea vulnerable y, por otro lado, mejorar la privacidad de nuestra cuenta con algunas buenas prácticas.

1. Protege la privacidad

Para proteger nuestra privacidad a través del correo debemos controlar quién dispone de la dirección de correo electrónico. Por eso, os recomendamos no utilizar la cuenta de correo que utilizamos para nuestro trabajo para suscribirnos a cualquier servicio de terceros. Si queremos probar programas, aplicaciones o plugins, lo mejor es tener una cuenta de correo alternativa para ello.

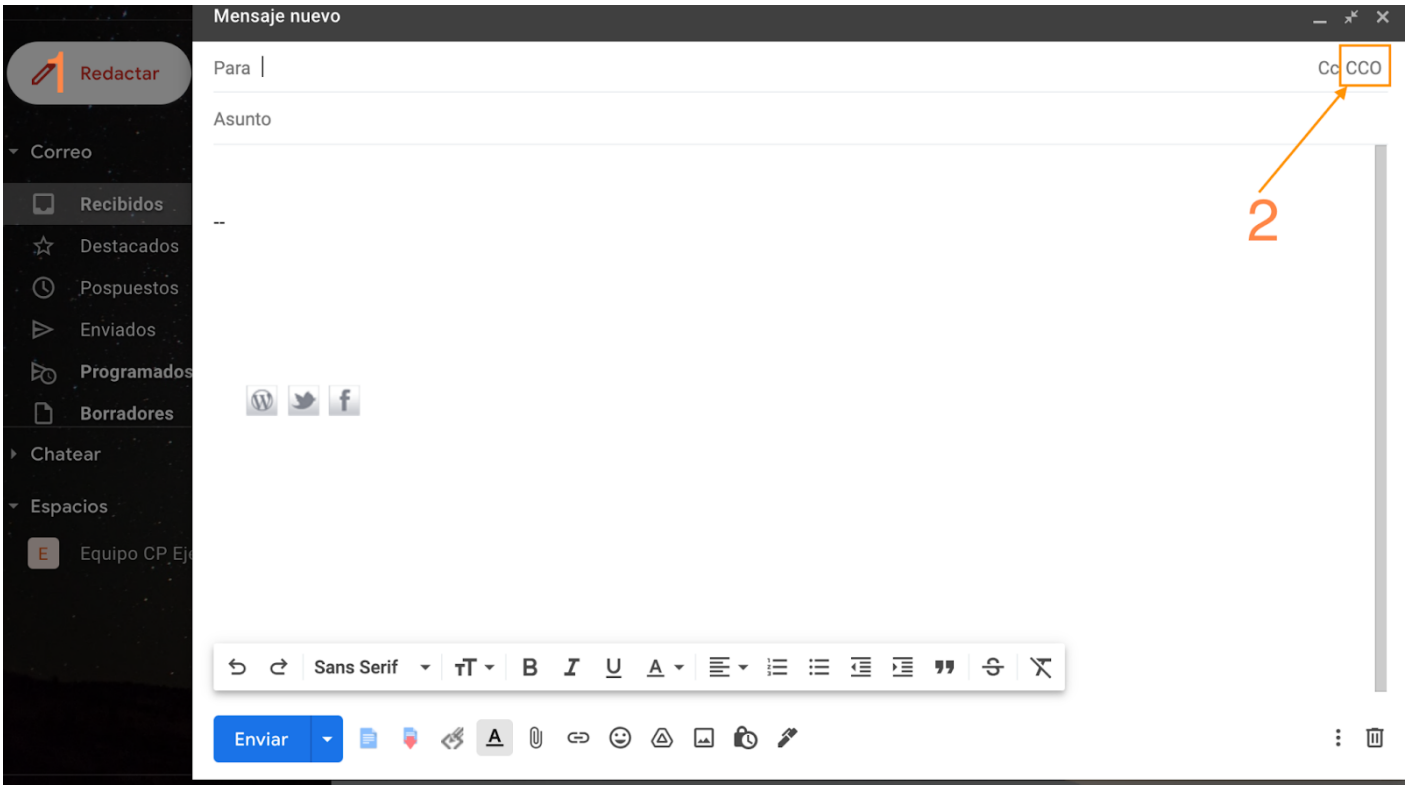
Si nos suscribimos a algún servicio, es necesario comprobar que el sitio sea confiable y tenga una política de privacidad respetuosa.

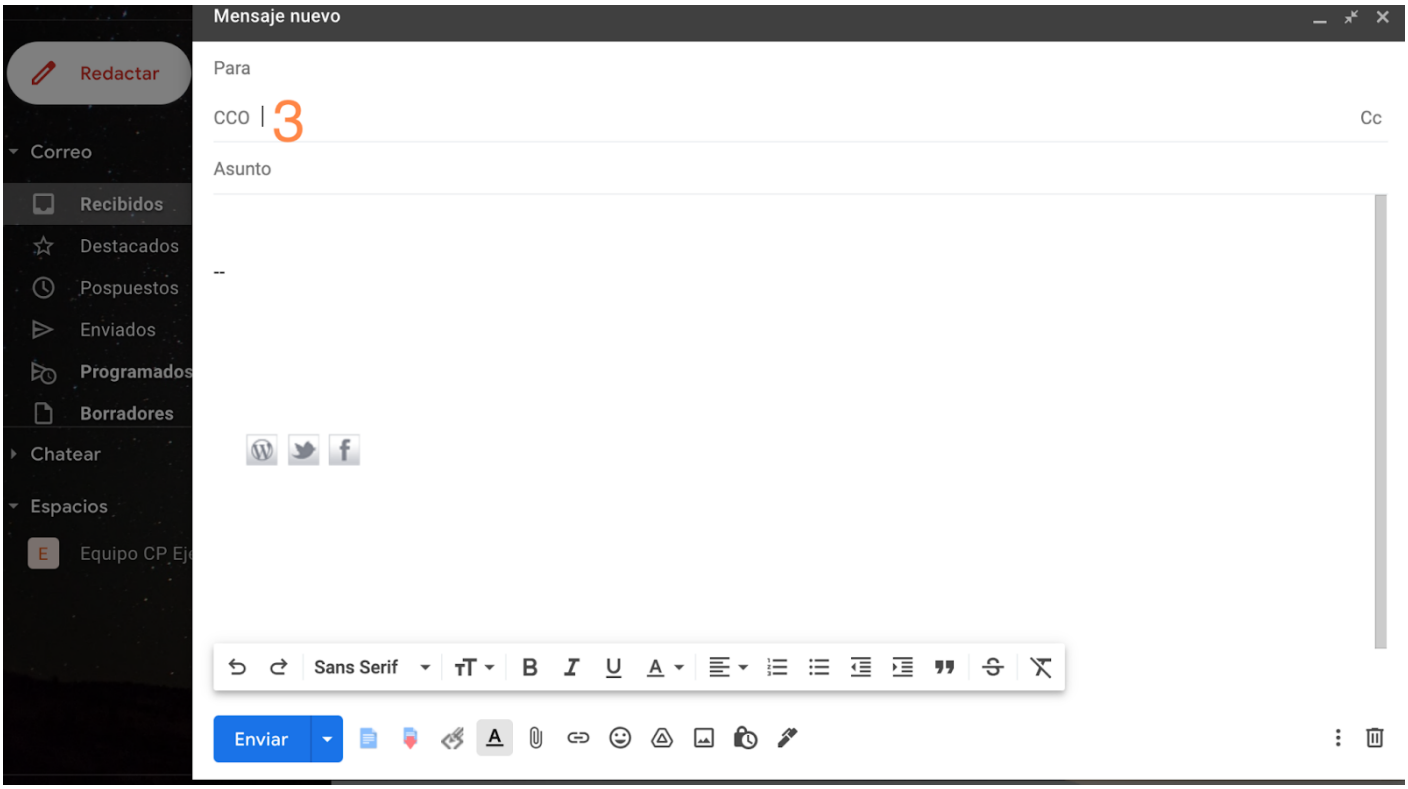
También podemos trabajar en favor de la privacidad de otros compañeros y compañeras con un simple gesto. Utiliza el campo CCO a la hora de enviar mensajes masivos, ya sea de forma interna entre el claustro o en las comunicaciones con las familias u otros colectivos. Ninguna familia tiene que enterarse del correo de otra a través de ti.

Para ello, hacemos clic en redactar. Nos aparece la ventana de redactar mensaje y en el lateral derecho tenemos las opciones de enviar en modo CC o CCO. Elegimos la segunda opción. De esta forma, quien reciba el correo sólo verá el correo del remitente, y no de los demás destinatarios.

Hacemos clic, y vemos cómo aparece el campo **CCO**, nos colocamos encima del mismo y agregamos los correos electrónicos de los destinatarios. Para añadir destinatarios, en Gmail podemos agregar un contacto, un grupo/carpeta o una lista de correos. Ponemos el nombre de correo, del grupo o de la lista, lo seleccionamos y se añadirán todos de forma automática. Si no sabemos el correo, podemos escribir la letra inicial del contacto y aparecerán todos los contactos

que empiecen por esa letra. Seleccionamos el deseado. Otra opción de agregar contactos es hacer clic en “**CCO**” y, en ambos servicios de correo, aparece una ventana emergente para realizar esa operación desde la herramienta “**Contactos**”, donde podremos buscar y seleccionar los contactos que recibirán nuestro correo electrónico.





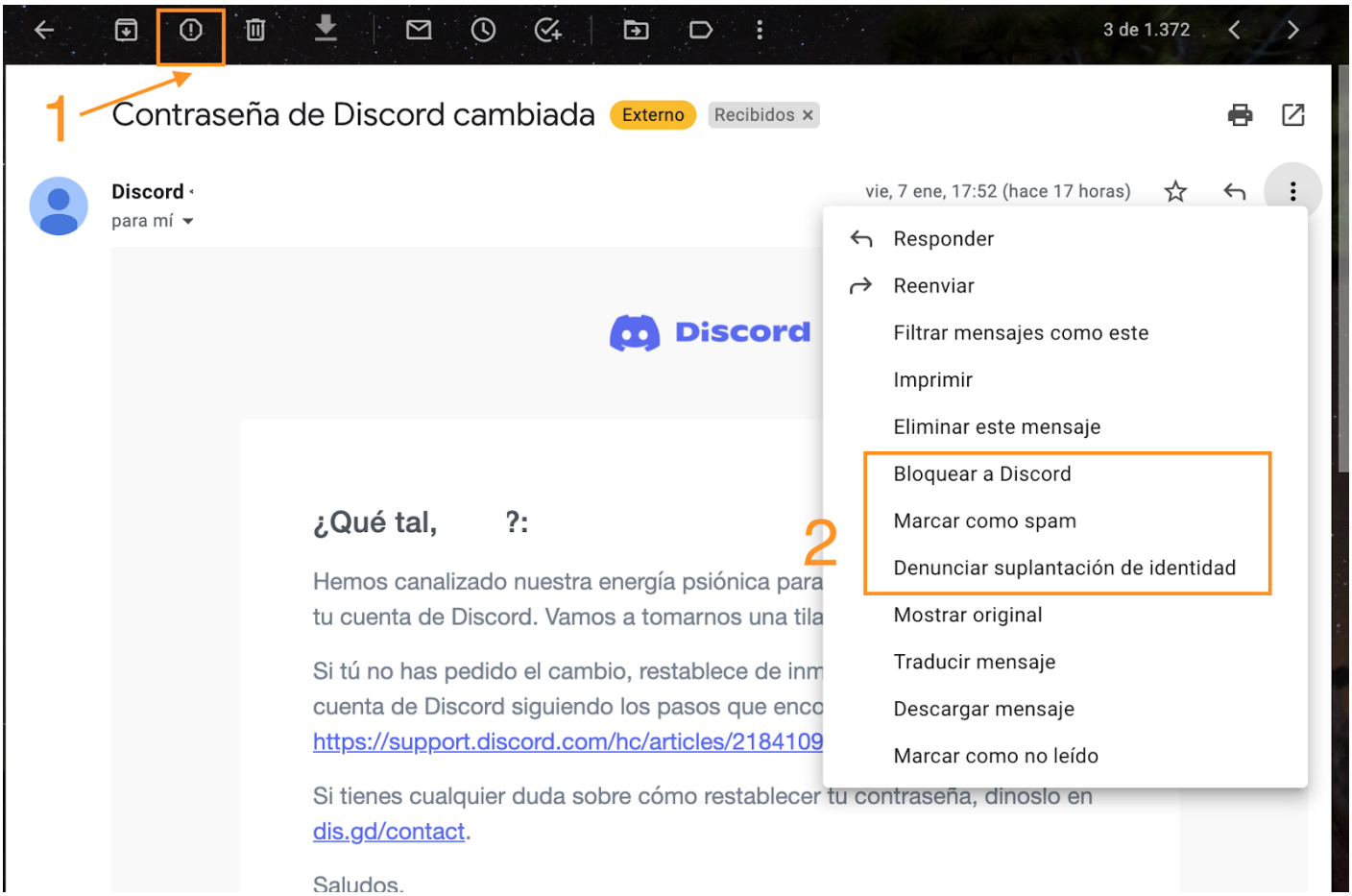
2. Cuidado con las cadenas o hilos

Una cadena o hilo de mensajes se produce cuando enviamos un correo a varios contactos y responden directamente a ese correo (generalmente responden a todos), de forma que en los correos más populares las respuestas se van anidando. si hay muchas respuestas, el mensaje original queda enterrado.

Las familias o alumnado no tienen, necesariamente, experiencia en el manejo del correo. Procura huir de los hilos o cadenas de mensajes largos, es preferible crear un nuevo mensaje que reutilizar otro anterior para responder.

3. Marca como Spam

Si recibes un correo no deseado de forma regular, es mejor que lo marques como spam (correo no deseado), ganarás tiempo. En Gmail es muy sencillo. Podemos seleccionar varios correos no deseados y hacer clic en "**Marcar como spam**" (1). O, una vez en el correo cuyo remitente deseamos marcar como spam, hacemos clic en el menú de tres puntos, se desplegará un submenú y elegimos la opción de Marcar como spam. También podemos bloquear al remitente del mensaje o, si creemos que tiene suplantar una identidad o tiene fines maliciosos, podemos denunciarlo.



4. Cuidado con el Phishing

Mahmoud Hassan, M. (s. f.). *Correos electrónicos de estafa* [Ilustración]. https://www.publicdomainpictures.ne. https://www.publicdomainpictures.net/es/view-image.php?image=281134&picture=correos-electronicos-de-estafa

Antes de abordar qué es el Phising, debemos recordar que, si tenemos **una cuenta de correo corporativa**, en este caso ligada de Google Workspace o si tenemos una cuenta de Microsoft TEAMS, o de cualquier otra plataforma, esa cuenta de correo **debería de utilizarse exclusivamente para nuestra labor en el centro educativo**. Para p**robar programas o cualquier otra cuestión personal es muy recomendable utilizar una cuenta personal** (o i**ncluso crear una cuenta sólo para registrarse** en páginas, servicios o para probar herramientas que deseamos utilizar en nuestra labor educativa). **Si utilizamos nuestra cuenta corporativa para esas tareas, estamos exponiendo esa cuenta** (y los datos que tenemos en ella) y puede ser víctima de prácticas como el Spam o el Phishing.

> El **phishing es una de las estafas con mayor trayectoria** y mejor conocidas de Internet. Es un tipo de fraude que se da en las telecomunicaciones y que emplea trucos de ingeniería social para obtener datos privados de sus víctimas. La diferencia entre Spam y Phishing es clara: el Spam es correo basura, no es más que un montón de anuncios no deseados. **El phishing por otro lado, tiene como finalidad robar tus datos y utilizarlos contra ti.**

Independientemente del medio, pues t**ambién se da esta práctica mediante SMS**, el atacante envía una comunicación con el fin de persuadir a la víctima para que haga clic en un enlace,

descargue un archivo adjunto o envíe una información (personal, bancaria, etc.) solicitada, o incluso para que complete un pago.

La **mayor parte del phishing puede dar como resultado el robo de identidades o de dinero, y también es una técnica eficaz para el espionaje industrial y el robo de datos**. "Algunos hackers llegan incluso a crear perfiles falsos en redes sociales, invierten un tiempo en desarrollar una relación con las posibles víctimas y esperan a que exista confianza para hacer saltar la trampa".

Un ataque de phishing tiene tres componentes:

1. El ataque se realiza mediante comunicaciones electrónicas, como un correo electrónico, un SMS o una llamada de teléfono.
2. El atacante se hace pasar por una persona u organización de confianza.
3. El objetivo es obtener información personal confidencial, como credenciales de inicio de sesión o números de tarjeta de crédito.

La Oficina de Seguridad del Internauta, nos da una serie de consejos para evitar ser víctimas de esta actividad fraudulenta:

Trucos para evitar ser víctima de phishing:

- Sé **precavido ante los correos** que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- **Sospecha si hay errores gramaticales en el texto,** pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- Si recibes **comunicaciones anónimas del tipo "Estimado cliente", "Notificación a usuario" o "Querido amigo",** es un indicio que te debe poner en alerta.
- **Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala seña**l. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.
- **Revisa si el texto del enlace que facilitan en el mensaje coincide con la dirección a la que apunta,** y que ésta corresponda con la URL del servicio legítimo.
- **Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas**. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.
- Aplica la **ecuación: solicitud de datos bancarios + datos personales** = fraude.

Fuente de este contenido y más información en:

Oficina de Seguridad del Internauta (s.f.). *Conoce a fondo qué es el phisin*g. https://www.incibe.es/aprendeciberseguridad/phishing

Belcic, I., *Guía esencial del phishing: cómo funciona y cómo defenderse*. Avast: https://www.avast.com/es-es/c-phishing

5. Autentificación en dos pasos

[Seguridad y privacidad]. (2021). https://www.pxfuel.com/. https://www.pxfuel.com/en/free-photo-oegsj

Ya estemos trabajando con nuestra cuenta de correo electrónico personal o corporativa, os recomendamos activar la autenticación en dos pasos. Esta tecnología está presente en los principales servicios de correo electrónico (también en redes sociales y otros muchos programas de comunicación o banca online).

La idea es simple: añadir una verificación más para certificar que quien accede a la cuenta eres tú y no otra persona quien está accediendo con tu cuenta de forma fraudulenta. Para ello, el servicio comprueba que realmente tienes algo (móvil, código, token) que sólo tú deberías tener.

No cabe duda de que la autenticación en dos pasos aumenta notablemente la seguridad en nuestras cuentas de correo electrónico. Aunque tu contraseña no sea segura y la hayan averiguado, si tienes activado en tu correo la autenticación en dos pasos nadie más que tú podrá entrar en tu cuenta.

En Google: Para activar la verificación en dos pasos en tu cuenta de correo electrónico con Gmail, es recomendable seguir la guía que nos ofrece esta compañía:

Manual soporte Google.

Página de Google dedicada a explicar este proceso

> **IMPORTANTE**: Sin duda, si debemos recomendar una aplicación de móvil para gestionar la verificación en dos pasos y que nos facilita este proceso es Google Authenticator (Android o IOS) o Microsoft Authenticator.

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

Revision #10
Created 2 February 2022 13:39:01 by Iván Heredia
Updated 17 January 2023 16:01:26 by Equipo CATEDU