

¡CUIDADO: RIESGO A LA VISTA!



El desembarco de las redes sociales en nuestras vidas ha modificado el modo de relacionarnos con el mundo. Por ejemplo, hasta hace poco, para mostrarle una foto a un amigo, primero teníamos que imprimirla, luego encontrarnos con él y, finalmente, mirarla juntos. Ahora es mucho más sencillo, ¿no? Este nuevo mundo, más virtual y menos personal, también modificó los riesgos a los que nos exponemos. Frente a nuevas reglas de juego, debemos *aggiornar* las precauciones para no exponernos a situaciones riesgosas.

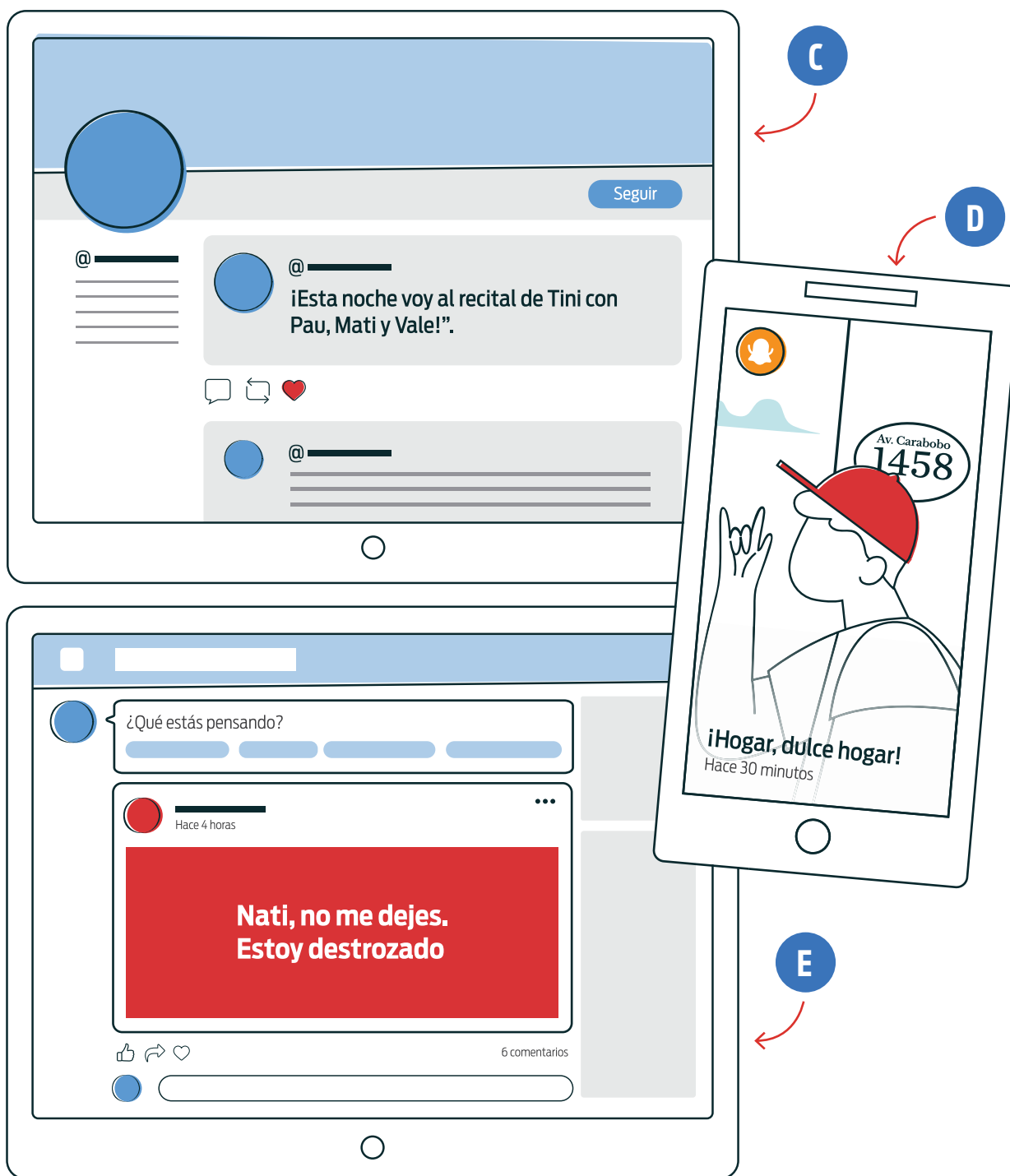
1. Observá las siguientes publicaciones en redes sociales y respondé las preguntas a continuación.



NOMBRE Y APELLIDO:

CURSO:

FECHA:



¿Qué tipo de información brinda cada imagen?

datos personales, ej: el de hogar dulce hogar se muestra como aparece la dirección de su casa.

NOMBRE Y APELLIDO:

CURSO:

FECHA:

¿Cuáles son los riesgos que podrían originarse a partir de cada una de las situaciones de las imágenes?

que te roben, secuestren , o que sepan donde estas

En cada caso, ¿la información sensible fue compartida voluntariamente?

yo creo que no fueron voluntariamente,exepcto la foto de las vacaciones y la ruptura

2. ¿Tenemos control sobre la información que publicamos en Internet? ¿Por qué?

a veces si y a veces no, por que puede cer que seamo sdescuidados y publicamos fotos o otras

cosas y no nos damos cuenta

NOMBRE Y APELLIDO:

CURSO:

FECHA:

LO QUE PUBLICO, ¿QUIÉNES LO VEN?

A veces es difícil imaginar hasta dónde puede llegar el contenido que publicamos en Internet. Por suerte, las redes sociales poseen configuraciones de privacidad que nos permiten decidir quiénes pueden ver nuestra información y quiénes no.



1. Contestá las siguientes preguntas, pensando en cada una de las redes sociales y aplicaciones que usás a diario. ¿Conocés la respuesta para todas ellas?

¿Quiénes pueden acceder a la información disponible en tu cuenta?

cualquier persona, lo que si no pueden por ejemplo acceder a tu cuenta de tik tok o de Instagram

y modifiquen: historias, videos, fotos etc.

¿A quiénes aceptás como contactos, amigos, seguidores, etc.?

¿Resultás fácil de encontrar y reconocer? ¿Tu nombre y/o foto de perfil es visible para todos?

¿Quiénes pueden escribirte por chat?

NOMBRE Y APELLIDO:

CURSO:

FECHA:

¿Podés bloquear cuentas de desconocidos que intenten contactarte o compartan contenido que te resulta agresivo o desagradable?

¿Cuánta información pueden ver otras personas sobre vos? ¿Todos pueden ver lo mismo?

¿Alguna de las redes sociales que usás se vincula con otras cuentas que uses? ¿Publica automáticamente lo que subís en algún otro sitio? ¿Te pregunta cada vez?

¿Podés ser etiquetado en publicaciones ajenas? ¿Quiénes pueden compartir tus publicaciones?

NOMBRE Y APELLIDO:

CURSO:

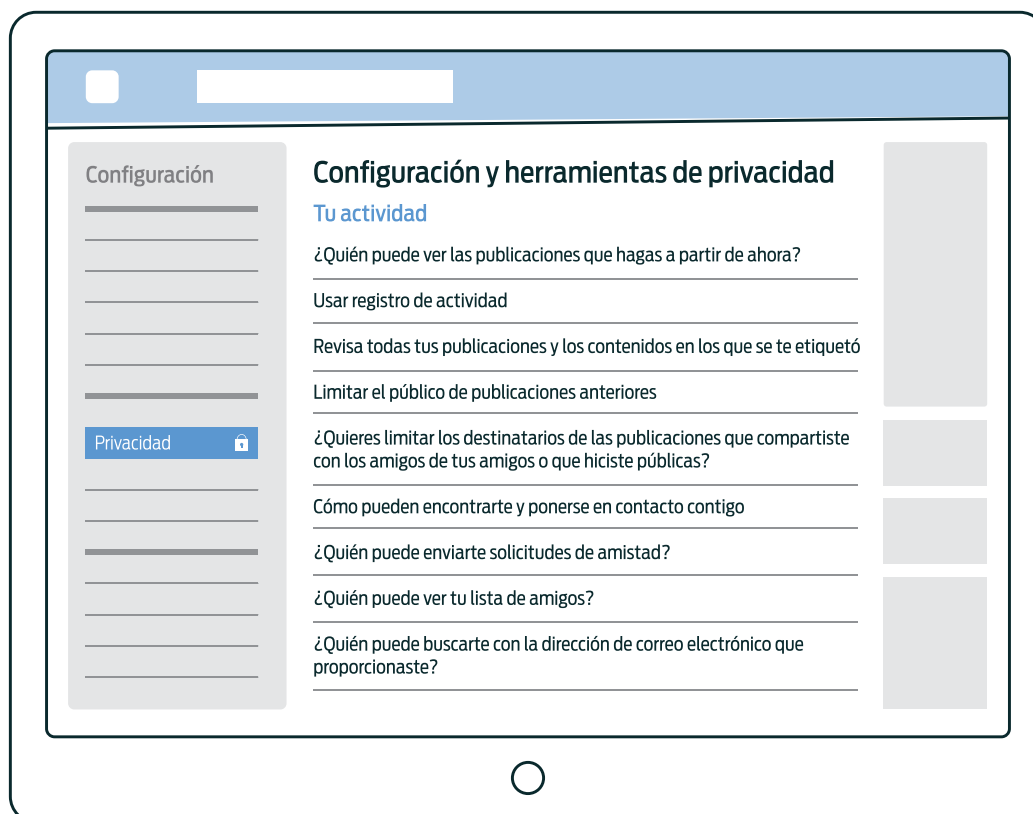
FECHA:

- 2.** Ingresá a las redes sociales con una cuenta que no forme parte de tus contactos y, una vez adentro, buscá tu nombre y apellido. ¿Con qué te encontraste? ¿Sabías que lo que ves está disponible para cualquier persona? Completá la siguiente tabla con tus hallazgos sobre la privacidad de tus datos en las tres redes sociales que utilices con más frecuencia.

RED SOCIAL	¿QUÉ ENCONTRASTE?	¿SABÍAS QUE ESA INFORMACIÓN ERA ACCESIBLE PARA CUALQUIERA?	¿QUERÉS QUE ESA INFORMACIÓN SEA ACCESIBLE PARA DESCONOCIDOS?

DECIDÍ VOS SOBRE LO PRIVADO Y LO PÚBLICO

Es importante que seas consciente de qué información compartís y con quién. Especialmente, a cuál pueden acceder desconocidos. Si bien las redes sociales permiten configurar el nivel de privacidad de lo que publicás, los niveles por defecto no suelen ser los más restrictivos. Revisá la configuración de tus cuentas y asegurate de que el alcance de tu información no vaya más allá de lo que vos querés.

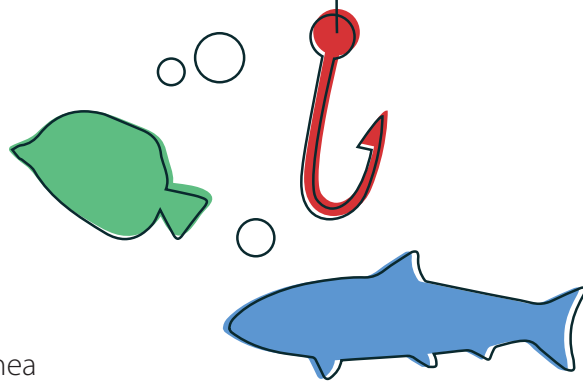


NOMBRE Y APELLIDO:

CURSO:

FECHA:

NO QUIERO SER UN PESCADO



Un pescador pone la carnada en el anzuelo y lanza la línea al agua. Luego, pacientemente esperará hasta que... ¡zaz! ¡El pobre animal mordió el anzuelo! Aunque suene difícil de creer, la pesca virtual existe, y también los pobres pescados.

1. Mirá la siguiente página.



¿Qué es esta página? ¿Para qué se usa?

2. Leé atentamente el siguiente artículo periodístico y respondé las preguntas que se presentan a continuación.¹

7 de agosto de 2017

25 de mayo: el pueblo al que le robaron \$ 3,5 millones con un aviso en Google

Parecía un día más. Un día alegre, en realidad, para este municipio de 40 mil habitantes. Porque en el partido de 25 de mayo, a 220 kilómetros de la Capital, después de mucha insistencia recibían una ambulancia para Norberto de la Riestra, una de las localidades de este partido bonaerense. [...]

La municipalidad

Aquel lunes 21 de noviembre de 2016, Roberto Testa, el tesorero del municipio, entró a trabajar a las 8 de la mañana en 25 de mayo, la ciudad que es cabecera del partido homónimo y que crece junto a la laguna Las Mulitas. A las 10, como todos los días, fue al Banco Provincia. Pidió que le imprimieran un resumen con todos los movimientos de las cuentas bancarias. [...] Ese día detectó, con su ojo prolijo de 32 años de carrera, que algo no andaba bien. "Empiezo y veo en el resumen que teníamos una transferencia por 100 mil pesos, otra por 90 mil. Me fui corriendo a lo del contador a comprobar por qué habíamos hecho esos movimientos", explica. [...]

El home banking

Paolo Salinas, el contador hace 18 años y encargado de emitir los pagos, giró su mirada hacia la puerta de la oficina para recibirlo. Escuchó a Testa y de inmediato se metió en las cuentas de *home banking* con su computadora. Salinas es el único que sabe las claves. Y no las anota en ningún lado, "por seguridad", dice. "Están en mi cabeza", acota. [...]

No recuerda específicamente el proceso de ese día, pero por lo general busca "Banco Provincia BIP" (Banca Internet Provincia) en Google, hace clic en el primer resultado, ingresa las claves y empieza a revisar las cuentas. "En ese momento me decía que había un usuario más adentro al mismo tiempo que yo", recuerda. Le preguntó a Romina Mancha, la subcontadora, si era ella. "No", le contestó Mancha desde el otro lado de la oficina, mientras dejaba su silla y se acercaba a la PC de Salinas. [...]

Mancha dejó el monitoreo y fue corriendo hasta la oficina de Ticera, la secretaria de Hacienda, quien a esa hora estaba reunida. No golpeó la puerta cerrada para entrar. "Me interrumpe y me dice: 'nos están robando, nos están robando' [...]", recuerda. [...] Fueron a buscar al Intendente: "Salimos disparadas". [...]

Tres millones y medio

El intendente, de 32 años [...], no salía de su asombro. Le pidió a Salinas que le mostrara lo que estaba sucediendo. Otra vez. Se dieron cuenta de que habían aparecido más transferencias, todas hechas a proveedores no habituales del municipio. "Cada segundo que pasaba perdíamos más plata", rememora. A esa altura, casi el mediodía de ese lunes fatídico, ya había 3 millones y medio menos de pesos en las arcas municipales [...]. Entonces, recibieron al menos una buena noticia: lograron que les bloquearan las cuentas. Eran poco más de las 12. [...]

¹ El artículo completo puede encontrarse en <http://bit.ly/2krwGH0>.

Pesca con mediomundo

Juan Ignacio Bidone es fiscal de investigaciones complejas del Departamento Judicial de Mercedes. A esta altura, tiene muy claro lo que pasó. La secuencia del robo de 3 millones y medio pesos al municipio de 25 de mayo, dinero que luego fue extraído de diferentes cuentas, se realizó mediante *phishing*: una forma de engaño informático con la que se logra que un usuario revele información personal. Los ciberdelincuentes crearon un sitio falso similar al de la Banca Internet Provincia, también conocido como BIP por sus iniciales. Era idéntico al verdadero, pero con un detalle: la dirección, que obviamente no puede ser la original. Suplantaron la a por la s, para hacer más imperceptible el cambio, y montaron un sitio en la dirección bancsprovincia.bancsinternet.com.ar.



El resultado falso que aparecía en Google

Para lograr que alguien visitara ese sitio pensando que estaba entrando al Banco Provincia aplicaron una técnica llamada *black hat SEO*: una estrategia que desafía las reglas para lograr escalar posiciones en los listados de Google. En este caso, contrataron el servicio publicitario de AdWords; eso fue determinante, ya que lograron hacer que ante una búsqueda en Google de la frase "Banco Provincia BIP" el sitio falso que crearon apareciera como primer resultado. [...]

Cuando alguien entraba, en el sitio falso se le pedía el nombre de usuario y la clave para ingresar a las cuentas del banco. Capturaba la información y luego redirigía al verdadero sitio BIP para no despertar sospechas. [...] Así —estima la fiscalía— los delincuentes se hicieron de las contraseñas, la única credencial necesaria para realizar la operación. [...]

¿Quién o quiénes fueron las víctimas del ataque descrito en el artículo?

¿Qué información fue robada por el atacante?
