

# A Positive Digital Footprint



What is a digital footprint? If your teenager uses the Internet, then he has one! His footprint is the trail he leaves online, including comments, photos, and chats. And his footprint is seen not only by friends and relatives, but also by potential employers and college admissions staff. Here are ways to help your teen project a positive image—and stay safe—when he's online.

.....

doesn't like, she could ask the site administrator or the person who posted it to remove it. (She can click on "About" or "Contact" to find the site owner.)

## List rules

Talk to your high schooler about how you expect him to behave online. For example, he shouldn't post inappropriate photos of himself or anyone else, and he shouldn't post personal information like his phone number or address. Together, make a list of rules and hang it by the computer or on the refrigerator to remind him about responsible and safe behavior. *Idea:* Consider having him sign a "usage contract" so you're both on the same page. Make your own, or find one at [fosi.org/good-digital-parenting/family-online-safety-contract](http://fosi.org/good-digital-parenting/family-online-safety-contract).

## Google yourself

To see what the world sees when searching her name online, encourage your teenager to type her name into Google or another search engine. She'll find links to any social net-

working profiles she has, product reviews she has posted, or mentions of her name in the news (for awards or sports results, for example). *Note:* If she sees anything she

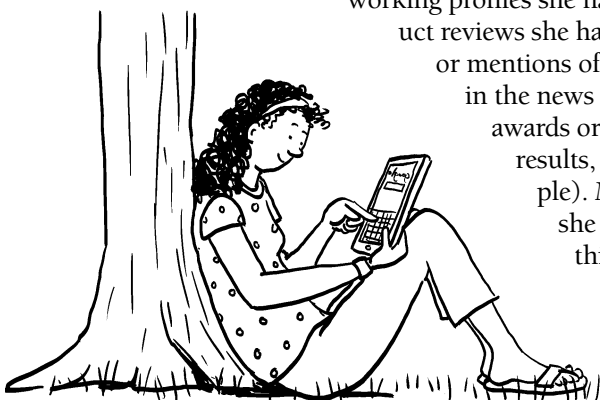
## Project a good image

What kind of impression does your high schooler want to make on people who view his accounts? Suggest that he cast himself in a positive light by posting polite reviews, retweeting good news, or congratulating a school sports team, for instance. On the other hand, he should avoid using bad language or making nasty comments. Let him know that bad grammar can hurt his digital footprint, too!



## Choose passwords wisely

Tell your teen to pick passwords that are difficult for others to guess. Keeping them secret can prevent people from accessing her devices and accounts and potentially sending or posting negative messages or charging purchases in her name. A combination of numbers and upper- and lower-case letters is much safer than her pet's name or her favorite color—things that others would know about her. She should also vary passwords across accounts, change them at least every three months, and keep any record of them in a safe spot (say, her desk drawer). Explain that she shouldn't share them with anyone besides you, not even her closest friends. If someone does learn a password, she'll need to change it right away.



*continued*



**Online is forever**

In this age of social networking, texting, and hacking, anything your high schooler posts or sends electronically may never go away—even if she deletes it. Point out that once she posts a comment or a photo, she should assume it's out there forever. Remind her that someone could have taken a screenshot of her post before she deleted it, an older version of the website may be available, or a hacker might steal information and repost it.

**Monitor app updates**

Have your teenager disable “automatic updates” on phone or tablet apps. Each time an app is updated, privacy settings might change, making his personal information and photos suddenly public. Instead, he can wait for a notification that an update is available. Then, he should read its latest sharing policy and change settings so he controls what others see about him.

**Click carefully**

Encourage your teen to be choosy about what she clicks on. The wrong link or attachment can put unwanted software on her device. Some of these programs steal personal information or even send messages on a user's behalf. Mention that she'd feel pretty embarrassed if an email she didn't write went to everyone in her inbox. To help guard against this, she should

keep protective software (anti-virus programs, adware removers) up to date and not click on pop-up or banner ads.

**Steer clear of cyberbullying**

Remind your high schooler that his real-life values (responsibility, kindness, respect) apply online and that you expect him not to participate in cyberbullying. That means thinking carefully about the text messages he sends and the comments he posts on social networks. Also, let him know what to do if he is bullied—he should tell you right away and block the sender. Depending on the post, you may need to contact the school or even the police.

**Say no to online dating**

More and more teenagers are using websites to find dates. Explain to your child that there's no way to know if people are really who they say they are. Besides, as she learns to form relationships, there's no substitute for getting to know someone face-to-face before deciding to date. When you set dating rules for her, include a rule against meeting someone in person whom she first met online.

**Watch out for identity theft**

Since teens are starting with a clean credit history, identity theft can go unnoticed for a long time—maybe even until your child applies for his first loan or credit card. Suggest that he check his bank account frequently for any unusual activity. Also, he could get a free credit report yearly from each of the three major credit bureaus (see *annualcreditreport.com*). *Note:* If someone has used his personal information to apply for or open an account, have him contact the bank or firm.



**Spend time “IRL”**

Limiting the amount of time your child spends using her phone or surfing the Internet will give her more time to interact with people in real life. Experts recommend no more than two hours of screen time per day for teenagers (not including homework).



Encourage her to balance screen time with real-life activities like hanging out with friends, playing sports, participating in extracurricular activities, or doing community service.

**High School Years**

# Una huella digital positiva



¿Qué es una huella digital? Si sus hijos usan Internet, ¡tienen una! Sus huellas son el rastro que dejan en la red e incluyen comentarios, fotos y chats. Y sus huellas las ven sus amigos y familiares pero también posibles empleadores y el personal de la oficina de admisiones de la universidad. He aquí formas de que sus hijos proyecten una imagen positiva—y protejan su seguridad—mientras están en la red.

.....

algo que no le gusta, podría pedirles al administrador del sitio o quien lo publicó que retiren el comentario. (Puede hacer clic en “About” o en “Contact” para encontrar al propietario del sitio.)

## Lista de normas

Hable con su hijo sobre cómo espera que se comporte en la red. Por ejemplo, no debería publicar fotos inapropiadas de sí mismo o de otras personas y no debería publicar información personal como su número de teléfono o dirección. Hagan una lista de normas y colóquenla junto a la computadora o en la nevera para que tenga presente el comportamiento responsable y seguro. *Idea:* Considere que le firme un “contrato de uso” para que tanto usted como él sepan a qué atenerse. Escriban el suyo propio o encuentren uno en [at fosi.org/good-digital-parenting/family-online-safety-contract](http://fosi.org/good-digital-parenting/family-online-safety-contract).

## Proyecta una buena imagen

¿Qué tipo de impresión quiere causar su hijo en la gente que ve sus cuentas? Sugíerale que ofrezca una buena imagen de sí mismo publicando reseñas positivas, reenviando buenas noticias o felicitando a un equipo de deportes, por ejemplo. Por otro lado debería evitar el mal lenguaje o hacer comentarios desagradables. Explíquele que la mala gramática también puede perjudicar su huella digital.



## Búscate

Para que su hija vea lo que el mundo ve cuando busca su nombre en la red, animela a que teclee su nombre en Google o en otro buscador. Encontrará enlaces a los perfiles que tiene en las

redes sociales, a las reseñas de productos que ha publicado o a las menciones de su nombre en la prensa (por premios o resultados de deportes, por ejemplo).

*Nota:* Si ve

## Elige bien las contraseñas

Dígale a su hija que elija contraseñas que otras personas no puedan adivinar con facilidad. Mantenerlas en secreto puede evitar que otra gente tenga acceso a sus aparatos y cuentas y que envíen o publiquen mensajes negativos o que realice compras a su nombre. Una combinación de números y letras mayúsculas y minúsculas es algo mucho más seguro que el nombre de su mascota o su color favorito, cosas que otras personas conocen de ella. Debería también tener distintas contraseñas para sus diversas cuentas, cambiarlas por lo menos cada tres meses y guardarlas en un lugar seguro (por ejemplo, en el cajón de su mesa). Explíquele que no debería compartirlas con nadie salvo usted, ni siquiera con sus amigas más íntimas. Si alguien averigua una de sus contraseñas, debe cambiarla inmediatamente.



continúa



## En la red para siempre

En la edad de las redes sociales, mensajes de texto y piratería digital, lo que su hija publica o envía electrónicamente se queda para siempre, aunque ella lo borre. Indíquele que una vez que publica un comentario o una foto, tiene que dar por sentado que estará allí siempre. Recuérdele que alguien podría haber hecho una foto de su post antes de que lo borrara, puede que exista una versión anterior del sitio, o un pirata digital podría robar información y volverla a publicar.

## Controla las actualizaciones de programas

Dígale a su hijo que desconecte las “actualizaciones automáticas” en los programas del teléfono o la tableta. Cada vez que se actualiza un programa pueden modificarse los controles de seguridad, convirtiendo de repente su información personal y sus fotos en algo público. Puede esperar en cambio a la notificación sobre la disponibilidad de una actualización. A continuación él debería leer los planes más recientes para compartir información y modificar los controles para gestionar lo que los demás ven sobre él.

## Haz clic con cuidado

Anime a su hijo a que seleccione bien los enlaces en los que cliquea. Un enlace o archivo equivocado puede instalar software indeseable en su aparato. Algunos de estos programas roban información personal o incluso envían mensajes en nombre de un usuario. Mencione que se avergonzará si un correo electrónico que no escribió

termina en el buzón de todas las personas de su carpeta de entrada. Para que se proteja de esto, debería mantener actualizado el software protector (programas antivirus, limpiadores de software de propaganda) y no hacer clic en anuncios electrónicos.

## Evita el ciberacoso

Recuerde a su hijo que los valores de su vida real (responsabilidad, amabilidad, respeto) son válidos también en la red y que usted se espera que no participe en ciberacoso. Esto implica pensar con cuidado los mensajes que envía y los comentarios que publica en las redes sociales. Explíquele también qué debe hacer si le acosan a él: debería decírselo a usted inmediatamente y bloquear al remitente. Dependiendo del post, quizá tengan que contactar con la escuela o incluso la policía.

## No a las citas en la red

Más y más adolescentes usan los sitios web para citarse. Explíquele a su hija que es imposible saber si la gente es quien dice ser. Además, cuando se inicia una relación, para conocer a alguien no existe un sustituto para el cara a cara antes de decidirse a salir con una persona. Cuando le dé normas para las citas, incluya una que prohíba verse en persona con alguien a quien conoció primero en la red.

## Atención al robo de identidad

Como los adolescentes empiezan con un historial de crédito limpio, es posible no darse cuenta del robo de identidad durante un largo tiempo, quizá hasta que su hijo solicita su primer préstamo o tarjeta de crédito. Sugíerale que verifique su cuenta bancaria con frecuencia para comprobar que no hay actividad rara. También podría pedir un informe crediticio gratuito anual de cada una de las agencias de crédito más importantes (vayan a *annualcreditreport.com*). *Nota:* Si alguien ha usado su información personal para solicitar o abrir una cuenta corriente, dígame que se ponga en contacto con el banco o la compañía.



## Tiempo para vivir

Limitar el tiempo que su hija pasa usando el teléfono o navegando por Internet le dará más tiempo para relacionarse con la gente en la vida real. Los expertos recomiendan que los adolescentes no pasen más de dos horas al día frente a la pantalla (excluyendo el tiempo con los deberes).



Anímela a equilibrar el tiempo que pasa frente a la pantalla con actividades de la vida cotidiana como salir con sus amigos, practicar deporte, participar en actividades extraescolares o haciendo servicio comunitario.

## High School Years