Company Overview:

Facebook is a social utility that gives people the power to share and makes the world more open and connected. The site has over 100 million active users from around the world, and more than 50 million people use Facebook every day.

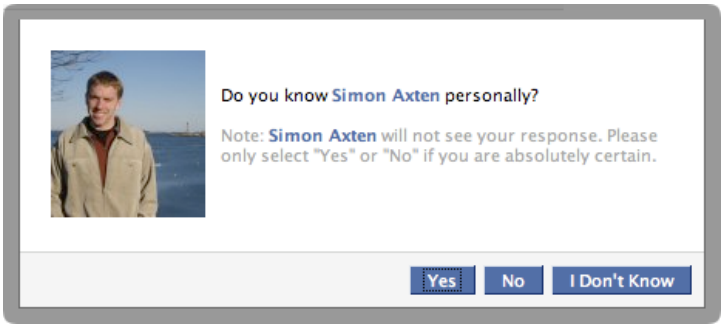
Relevant URLs: www.facebook.com
www.facebook.com/privacy
www.facebook.com/help.php

1. The principal safety issue Facebook works to address is anonymity. While appropriate in some settings, fake names and hidden identities are incongruous with Facebook's goal of allowing people to share and communicate more openly and efficiently. When users are allowed to misrepresent themselves, trust and accountability break down, and people feel less confident in their interactions. Bad actors are emboldened because there is little chance of serious consequence. Most of the systems and processes we have developed are intended to solve this root problem, and we measure the risk that youth face on our site by how well we are doing in this effort.

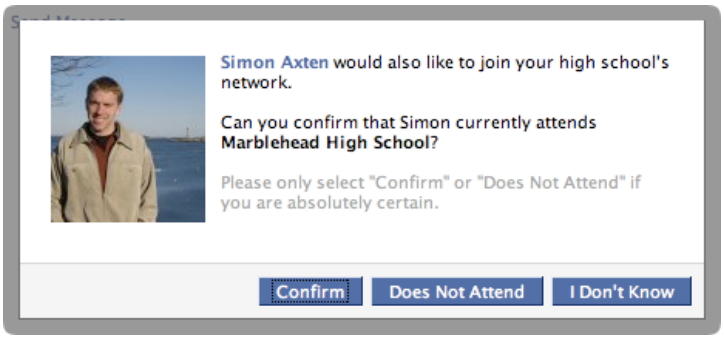
2. Facebook's network-based architecture strives to reflect as closely as possible real world social communities. By default, users' profiles are only available to those who share networks with them or have been confirmed as friends.

   We provide extensive and particular privacy controls that allow users to specify what information they make available and to whom. Users can restrict access to their profile to confirmed friends only, and can even create lists of people from their larger friend group to tailor privacy further.

   Facebook employs a system of peer verification for users who identify themselves as under 18. This system relies on answers to questions accompanying friend requests to help determine if the user sending those requests attends a particular high school or knows the people he or she is contacting. Accounts are either verified or disabled based on these answers.

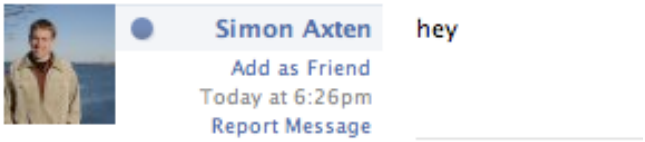


   A high school network affiliation must be established through the process above before a user can gain access to the profiles of others on that network. Users must be 18 or under to join a high school network.



Regional networks are segmented by age. By default, minors cannot see the profiles of adults on the same regional network, and vice versa. Adults also cannot browse for minors based on profile attributes.

Users can report suspicious content or behavior using the report links located throughout the site. They can also use the contact forms on our Help page or send an email directly to one of our several aliases, which include info@facebook.com, privacy@facebook.com, and abuse@facebook.com.



We are committed to reviewing all user reports of nudity, pornography, and harassing messages within 24 hours and resolving all email complaints sent to abuse@facebook.com within 72 hours.

We have developed several automated systems to detect anomalous behavior and block or disable the accounts of potential bad actors. Obviously, we must keep the signals these systems use confidential, but they generally look for unusual patterns in activity, and interactions between non-friends are looked at much more closely than those between friends. Some examples of things these systems look for are users whose friend requests are ignored at a high rate, or users who are contacting lots of people not on their friends list. They also look for adult users who are contacting an inordinate number of minors.

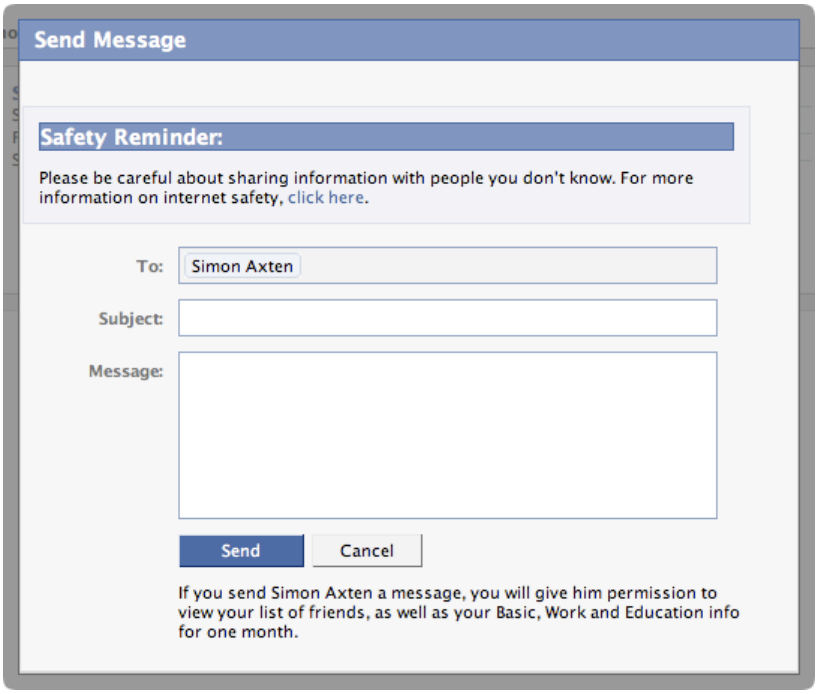
People who try to sign up with a birth date that makes them under 13 are blocked, and a persistent browser cookie is used to prevent further attempts at sign-up.

Users cannot edit their birth date to one that makes them under 18 without first contacting our User Operations team for review.

Facebook maintains an extensive blacklist of words likely to be associated with fake accounts, which is then used to block these accounts at sign-up.

Users cannot change their names without first submitting the change for approval. This is done through an algorithm that uses our blacklist and other factors to identify likely fake names.

Users under the age of 18 are shown a safety reminder any time they receive a message from, or begin composing a message to, an adult user with whom they have no mutual friends. This reminder tells them to be careful when sharing information with people they do not know, and provides a link to Facebook's Safety page.



Facebook has developed several automated systems to detect and disable fake accounts based on anomalous behavior, and is constantly working to improve these.

We disable the accounts of convicted sex offenders and work closely with law enforcement in cases where a minor has been contacted inappropriately, or where a user has committed a crime. We also plan to add the KIDS Act registry to our many existing safeguards and to use the database as vigorously and comprehensively as we can. Specifically, we will check new users at sign-up and review existing users as regularly as the technology allows. Anyone on the list will be prevented from joining Facebook. Anyone already on Facebook who is added to the list will have his or her account disabled. We will also continue to enhance our partnership with law enforcement to find and prosecute sexual predators who violate this new law with fake names, addresses, or handles.

We are working with Attorney General Milgram of New Jersey to test a different version of our report link in order to see what effect it has on the volume and quality of reports. We have also been working closely with Attorney General Cuomo of New York and Kroll, our independent safety and security examiner, on safety issues.

All of the above efforts are in-house. Facebook employs a team of User Operations analysts to resolve user reports and respond to complaints, as well as team of Site Integrity engineers to develop and fine-tune our automated systems.

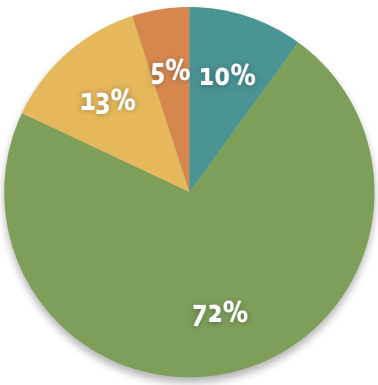
We are deeply committed to our own efforts in this area and believe the controls and processes we have built are leading the industry. At the same time, we recognize that protecting children online is an ongoing battle that requires cooperation among various groups, and we are always open to working with outside companies that have developed smart solutions.

3. Facebook tracks data on all of its automated systems, as well as on reports and complaints we receive from users and the actions we take on them. While we cannot provide specific numbers, we do receive hundreds of thousands of contacts each week. These include reports of nudity, pornography, and harassing messages, which we resolve within 24 hours. Our 100 million active users take great pride in keeping the site clean and are quick to report content and behavior they find offensive or threatening. Our quick response time in dealing with these reports has kept dangerous users off the site, and the very low number of serious incidents involving adults and minors who have met through Facebook is a testament to this.

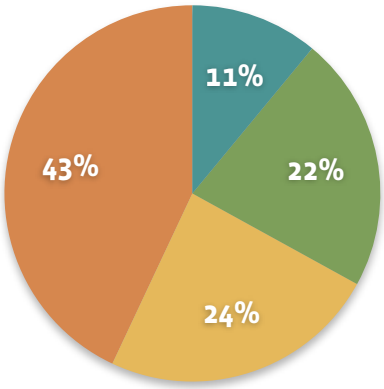
   We have also used our own Polling feature to gauge how minors are using the site, as well as how safe they feel on Facebook relative to other sites and the Internet at large. The results of a few of these polls, which use a sample of 500 users in the US aged 13-17, are below:

Have you ever seen nudity…

…on Facebook?



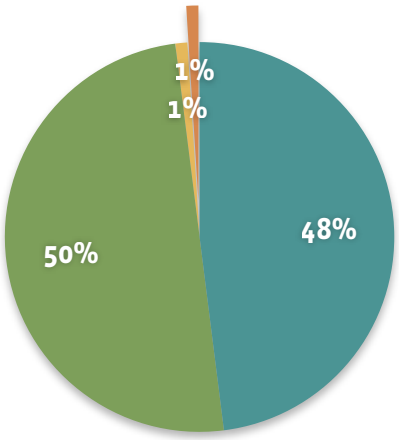
…on a website other than Facebook?



Green – No, never.
Yellow – Yes, a few times.
Orange – Yes, more than a few times.
Blue – I don't know.

These results show how effective our systems and processes are at keeping bad content off the site. Teens are much less likely to encounter nudity on Facebook than they are elsewhere on the Internet.

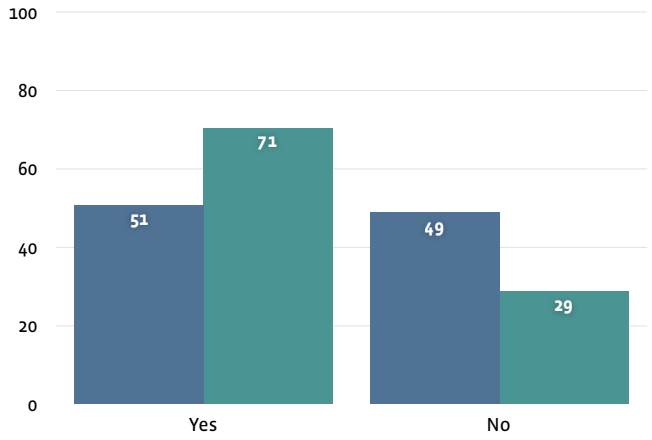
Do you know the people you interact with on Facebook in real life?



Green – Yes, most of them.
Blue – Yes, all of them.
Yellow – No, only a few of them.
Orange – No, none of them.

This poll shows that the vast majority of teens are using Facebook to communicate with people they already know in the real world. Because they are conditioned to use the site in this way, they are less likely to engage with a stranger on Facebook who might do them harm.

Have you ever used Facebook's privacy settings to limit access to your information?



Blue – Male
Green – Female

In fact, 100% of teens use our privacy controls because of the defaults we have put in place. This poll shows that 63% edit their settings even further, with girls using these controls slightly more often than boys.

In working to keep kids safe on Facebook, we have learned that technical solutions are imperfect, and that systems must be evaluated and refined on a regular basis to remain effective.

On the one hand, these systems must be focused enough not to produce a high rate of false positives. Controls meant to protect people will inevitably block some legitimate behavior. Our name blacklist, for example, prevents people with unusual names, or names shared by celebrities or other public figures, from signing up. These people must contact our User Operations team and prove their identity in order to create an account on the site. Likewise, our various systems for detecting anomalous behavior occasionally block or disable the accounts of people who are using the site in benign, but unanticipated and perhaps unintended, ways. The key is to establish an acceptable threshold for misses and then use these to inform and improve systems where possible. Because Facebook is a utility for sharing and communicating more efficiently, we must be careful not to restrict the power of the tool any more than is necessary to protect our users.

On the other hand, real bad actors are creative, and they quickly adapt and develop new methods when controls are built to block them. Facebook works hard to anticipate these changes and to quickly identify new dangerous behavior so that it can be stopped.

4. Unfortunately, we cannot provide specific details about our plans for the future. More generally, though, Facebook's mission, as well as our values of authenticity and control, will continue to guide the product. We will continue to develop and refine systems that discourage interactions between strangers, and encourage those between people who know each other in the real world. We are particularly focused on developing new ways to identify fake accounts and suspicious behavior, which will help us maintain the integrity of the social graph while improving safety and protecting our users from annoying phishing and spam attacks. As mentioned above, Facebook has been a strong supporter of the recently passed KIDS Act, and we plan to use the registry it creates to keep sexual predators off Facebook.

5. Once again, we have learned from experience that technical solutions, while helpful, are imperfect and must be accompanied by education and manual processes in order to truly be effective. Facebook has taken a multi-faceted approach to the problem of protecting kids online, using automated systems where they make sense, but also educating users on safe practices and staffing a responsible team to quickly review and respond to serious reports of misconduct. We have consistently found that blunt, heavy-handed approaches are the least effective, as they prevent legitimate use of the tool or service and provide bad actors with numerous options for circumventing controls.

Instead, Facebook recommends smarter, more focused systems that aim to block dangerous behavior while disrupting legitimate communication as little as possible. That being said, the very nature of the problem requires constant evaluation and refinement of these systems, as the behavior of both legitimate and bad actors can change over time. We believe that technical solutions should be focused primarily on the use of false identities and communication between people who do not know each other in the real world.