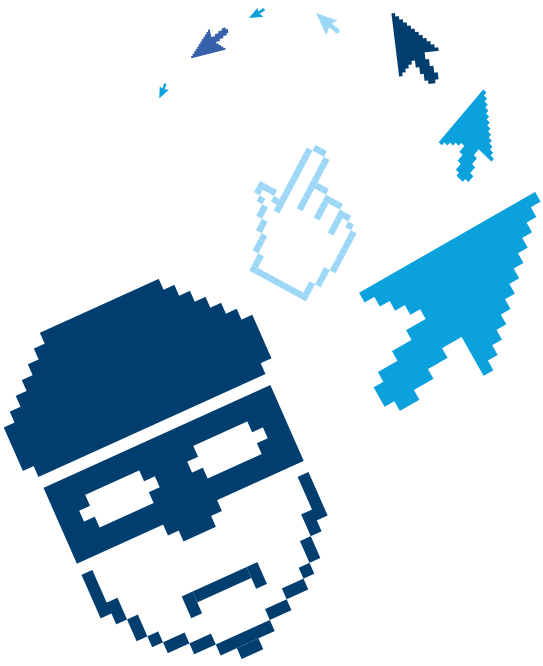
3 Social Media Habits to Implement Today

From personal thoughts and holiday photos, to social check-ins and ... well, just about anything ... very few day-to-day activities seem to be "off limits" when it comes to social sharing. And whether or not you agree or disagree with the fact that previously private moments are increasingly being shared online in the social sphere, the fact remains that you (and your family members and friends) are likely to be impacted by this shift in some way or another.

proofpoint.

Though it's easy to focus on the positive aspects of connecting online, there are plenty of hazards associated with these very public platforms. To reign in your risk, adopt the following three habits (and encourage others to do the same):



Tip #1: Regularly Review Your Privacy Settings

If you've never checked the privacy settings on your social media accounts, there's no time like the present. (And if you have younger kids who are on social media, check theirs while you're at it.) Though some platforms—like Twitter and LinkedIn—are designed to have a more public image and function, other platforms—like Facebook, Snapchat, and Instagram—thrive on person-to-person exchanges. It's critical that you understand how data privacy works within each of your social networks and that you choose your account settings appropriately.

A few things to keep in mind:

- Don't assume standard privacy safeguards are strong enough. Many applications default to less secure privacy settings in order to make your profile and posts easy to find and engage with.
- Social engineers and cybercriminals mine social networks for personal and business information. When you share data publicly, be aware that scammers can use those details against you to make malicious emails, phone calls, and other communications seem legitimate.
- Keep in mind that online privacy policies and settings change over time. It's a good idea to regularly check your settings, particularly following an update to a social media application that you use.

proofpoint.

DELETED POSTS AREN'T NECESSARILY GONE. "PRIVATE" MESSAGES WON'T NECESSARILY REMAIN PRIVATE. AND POSTS YOU THINK WILL "SELF-DESTRUCT" AFTER A FEW SECONDS ON A PLATFORM LIKE SNAPCHAT WILL NOT NECESSARILY DISAPPEAR.

Tip #2: Assume Everything You Post Is Public

This may seem in direct contrast to the first point, but such is the double-edged sword of social networking. The simple reality is that data privacy settings can only protect you to a point. When you share something with someone, that something is no longer in your control.

Think of social media posts like text messages: Once you send a text to someone, what's to stop that person from forwarding the message on to others? Or from taking a screen shot of that message and posting it on a social network? And what if the people who see that message then share it with their connections? This hypothetical (but common) chain of events shows that, even if a text message is intended to be a private exchange between you and the person you send it to, there are no privacy restrictions on messages once you hit send.

The same principles apply to social media. Deleted posts aren't necessarily gone. "Private" messages won't necessarily remain private. And posts you think will "self-destruct" after a few seconds on a platform like Snapchat will not necessarily disappear.

We have seen these realities play out in the media countless times, with deleted "controversial" tweets living on in screen captures. And it's not just scam artists who monitor social channels. More and more admissions officers and employers (both prospective and current) admit to making decisions based on the information they find on social channels. As such, it's to your advantage to assume that everything you post could travel well beyond the privacy confines you believe you've set.

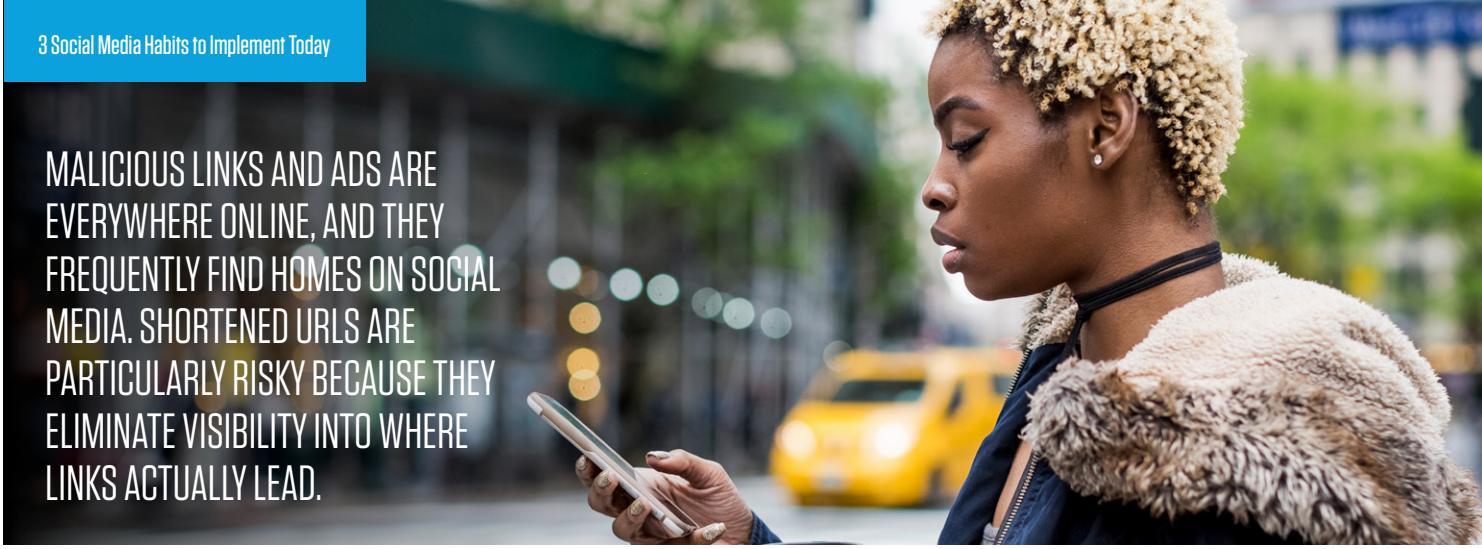
Tip #3: Ask Questions

We've said it already, but it's worth repeating: Scammers and cybercriminals love social media. Social accounts hold treasure troves of personal information, and it's incredibly easy for individuals to pretend to be someone or something they aren't within these networks. The dangers associated with imposters and fraudsters are real. There are financial threats, reputations at stake, and even risks to personal safety.

Before you click a link, accept a connection request, or download a file, take a moment to think about the implications if the person on the other end of the post or message has a malicious intent. These are the sorts of questions to ask yourself:

Do I personally know this individual and/or trust this connection?

The safest rule of thumb on social media (and a great piece of advice for minors) is to refuse connections from anyone you haven't met personally. That isn't always possible (particularly on Twitter), but it always makes sense to think about the information you share with your social connections. Most privacy settings focus on protecting your data from the prying eyes of those outside your accepted circle. All bets are off with those who have been granted access.



Am I already connected to this person?

Social media accounts are frequently the target of imposters, and it's likely you've been made aware of cases in which friends' accounts were either compromised (because of a password breach) or duplicated. Perhaps you've even experienced this yourself. If you suspect something like that is going on when you receive a request, check with your friend or report the suspicious activity before making the connection.

Does this seem legitimate?

From promises of free gift cards and access to premium content, to teasers about sensational stories and the latest celebrity gossip, there is a lot of so-called "click bait" on social networks. Scammers create fake profiles and business pages (a practice known as "pretexting") and use known brand names, incredible offers, and dramatic headlines to lure you in. Steer clear of too-good-to-be-true traps. (And don't be the one who shares the scammers' links for them!)

Also take notice if a friend suddenly starts posting odd things (like multiple ads for high-end sunglasses) or randomly asks you for money or information. Social media accounts are hacked regularly, and the hackers often blast out posts and messages looking for a quick score. If you suspect an account has been breached, reach out to your friend through another trusted channel (like a text, phone, or email message) or report the account.

Do I know for sure this link/file is safe?

Malicious links and ads are everywhere online, and they frequently find homes on social media. Shortened URLs are particularly risky because they eliminate visibility into where links actually lead. These abbreviated links are often used by reputable companies to ensure posts meet character count or display restrictions. But they are also used by fraudsters to mask the true destination of a link.

Bottom line: Confirm before you click. Whether full-length or shortened, seemingly innocent links can get you into a lot of hot water. If something seems off, avoid it. You should be as cautious on social media as you are with emails.

Am I teaching my kids to police themselves?

If you have children, it's always a good idea to check in on what they're doing online and the connections they are making. But it's an equally good idea to be proactive about social media safety. Teach them how to apply best practices themselves — and instruct them to ask questions and come to you if they are unsure about something.

Because our human tendency is to be trusting and open, it's important we all learn how to balance social sharing and safe sharing. Online safety can feel like a moving target, but these social media tips, which offer relatively basic precautions, can drastically improve the security of your personal information.