The Blinding Effect of Security Hubris on Data Privacy

Provided by

Malwarebytes LABS

Executive summary

In the humble early days of the Internet, anonymity was a comforting given. Most people used the world wide web to look up information or communicate with complete strangers under pseudonyms. They'd then return to their "real life" and conduct their business at the office, pay their taxes with an accountant, and buy clothes at the mall.

Today, real life and Internet life are blended into one. More often than not, users must include their full names, addresses, payment details, and vital financial data when they interact online. It's no surprise, then, that with each begrudging entry of sensitive personal information, not to mention each news story about companies such as Facebook and Google abusing that personal information, users are having an emotional reaction to data privacy.

What is surprising, however, is that their behavior does not match up with their feelings. From January 14 to February 15, 2019, Malwarebytes Labs conducted a survey on nearly 4,000 participants to measure respondents' confidence in their own privacy and security practices, as well as their confidence in privacy being maintained by businesses. And while data privacy was a top concern, with trust in companies to maintain it painfully low, users did not follow through with some of the more difficult and cumbersome cybersecurity best practices to keep their data safe.

Which had us begging the question: Why not?

An easy answer to that is, of course, that these practices are more difficult and cumbersome, so people avoid having to do them. However, if data privacy is so important to such a large number of respondents, and trust is so low in other companies to do it, why are people shirking the responsibility?

After analyzing responses from participants in Generation Z up to baby boomers, our findings show that perceived confidence in privacy practices is higher than reality. We determine this gap between perception and reality to be a result of security hubris. Because users follow many of the perceived-as-easier security tactics, they believe themselves safe, even while ignoring other important security measures that appear difficult.

This security hubris, however, is dangerous in today's climate, as cybercriminals and shady application developers alike identify those blind spots and use them to their advantage. Meanwhile, search engines and social media companies continue to abuse and misuse data its user perceive as private, such as their browsing habits and personal information.

Let's dig a little deeper into the data to see why the perception is not aligning with reality, and what, if anything, users can do to plug the gap.

The results

Most of our respondents practice good security hygiene. A vast majority (96 percent) of respondents in all generations care about their privacy, and 93 percent use security software. However, while users focus heavily on obvious security practices, they are frequently ignoring steps that protect against many common attack avenues.

We begin our analysis of the responses with the simple question: How important is protecting online privacy?

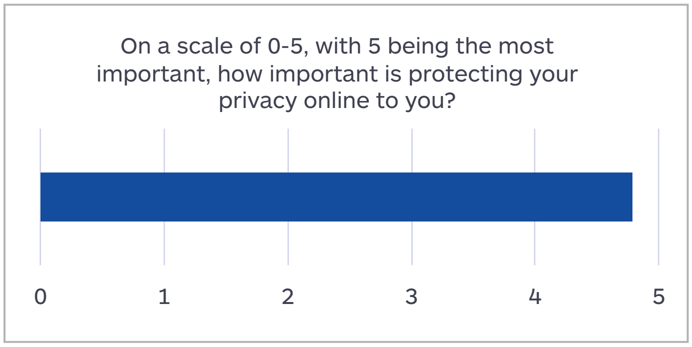

Figure 1. How important is protecting privacy online to you?

Our respondents' answers show that they are definitively invested in protecting their privacy. An overwhelming majority (more than 93 percent) of Millennials feel that it's important to protect their privacy online.

When we asked users if they take steps to protect privacy, we received an overwhelmingly positive response, although a small portion did admit to taking no steps at all.

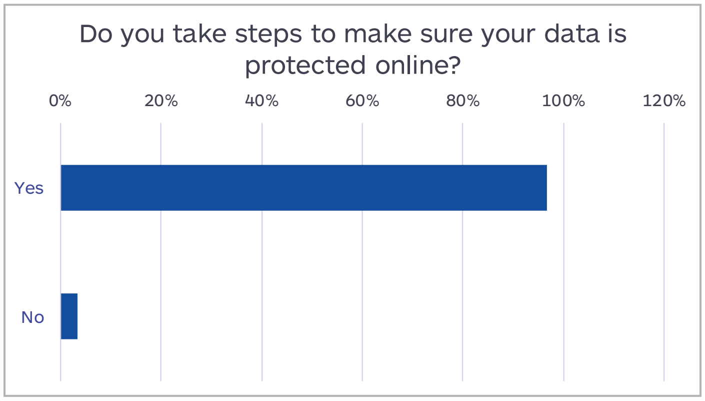

Figure 2. Do you take steps to make sure your data is protected online?

This indicates that users not only feel passionately about the importance of privacy, but that they believe they take action to support their emotional response. However, when asked about which specific steps they have taken to secure their privacy, we can see how those behaviors break down, depending on the task.

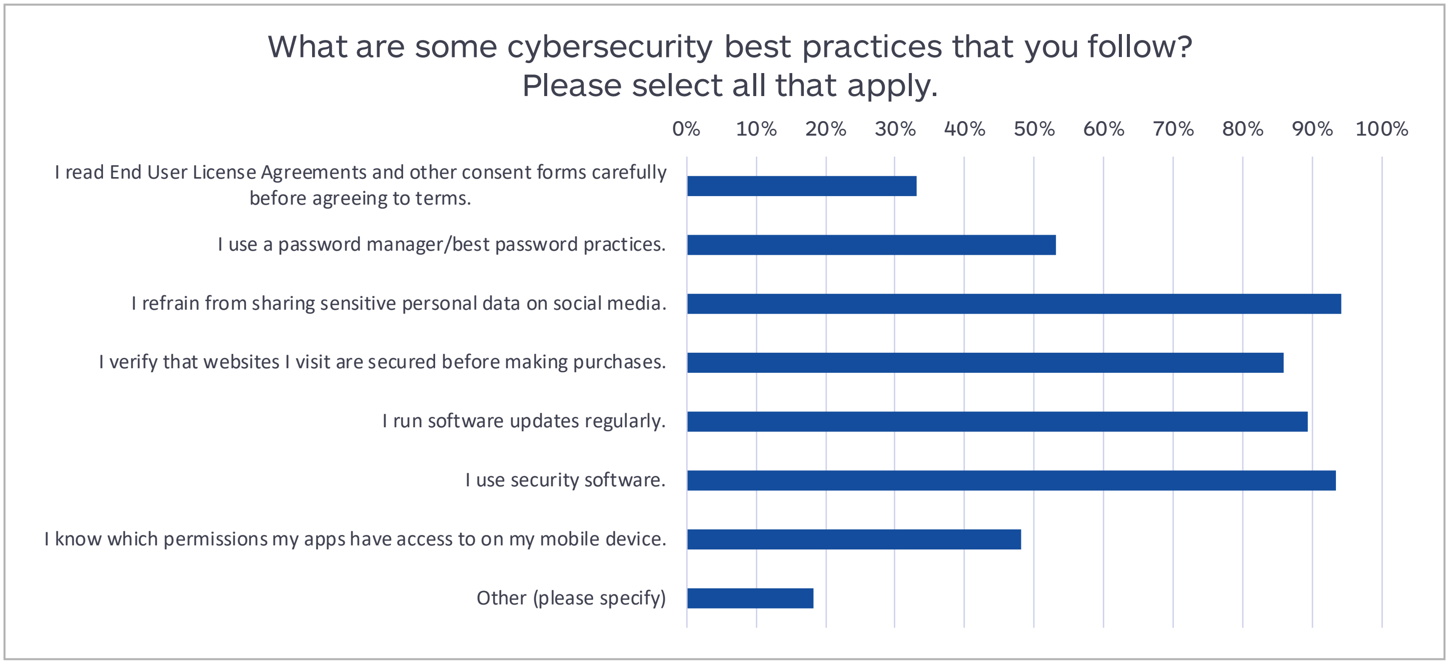

Figure 3. What are some cybersecurity best practices that you follow?

Where users are getting it right: They use security software, run updates regularly, verify that websites are secure before making a purchase, and refrain from posting sensitive personal information on social media. The most common responses were the use of security software and being cautious about what information is being posted online. However, note that only 32 percent read EULAs, 47 percent know which permissions their apps have, and a little more than 53 percent use password managers. Even with the use of security software, there's still room to improve general security and privacy practices.

To confirm our suspicions, we next asked what security practices our respondents do **not** follow.

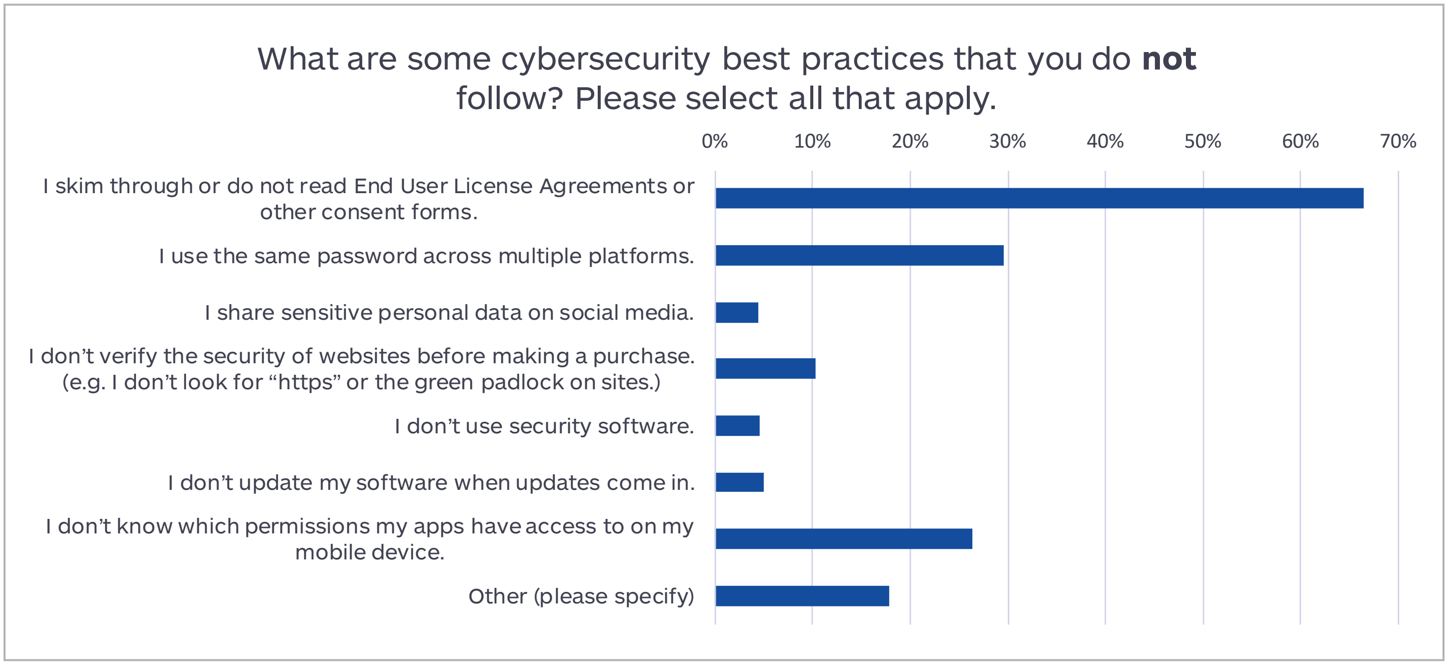

Figure 4. What are some cybersecurity best practices that you do NOT follow?

Sixty-six percent of users say they simply skim through or do not read End-User License Agreements or other consent forms.

The EULA document is usually incredibly long and full of technical and legal jargon. That is where the developers of potentially unwanted programs (and totally unwanted programs) hide agreements to sell your data to third parties or install additional software without your knowledge.

The next most common security fail (but still only at about 29 percent) is using the same password for multiple sites. Millennials are much worse at this practice—37 percent reuse passwords. This kind of behavior is what criminals want users to do. It makes it easy to steal the credentials from one source and use them elsewhere. Using a password manager is a great solution for this problem.

Finally, about 26 percent of respondents claimed they didn't know which permissions their apps had access to. This is a common issue that criminals and shady developers have taken advantage of in the past, like creating a flashlight app that needs access to your contacts for some reason.

The common factor between all three of these "not-followed" practices is that they are difficult to do correctly. EULAs are long and boring, passwords are hard to remember, and the user just wants to use the app already—why bother with permissions?

Security hubris makes us believe that since we are secured in one way, then we are secured in all ways. Who cares about passwords when you're careful about what you post on Facebook?

Blind faith in anything is dangerous; even the tools you put your faith in to keep you secure have drawbacks.

Further insight is gained through a following question on how comfortable users were with sharing data online.

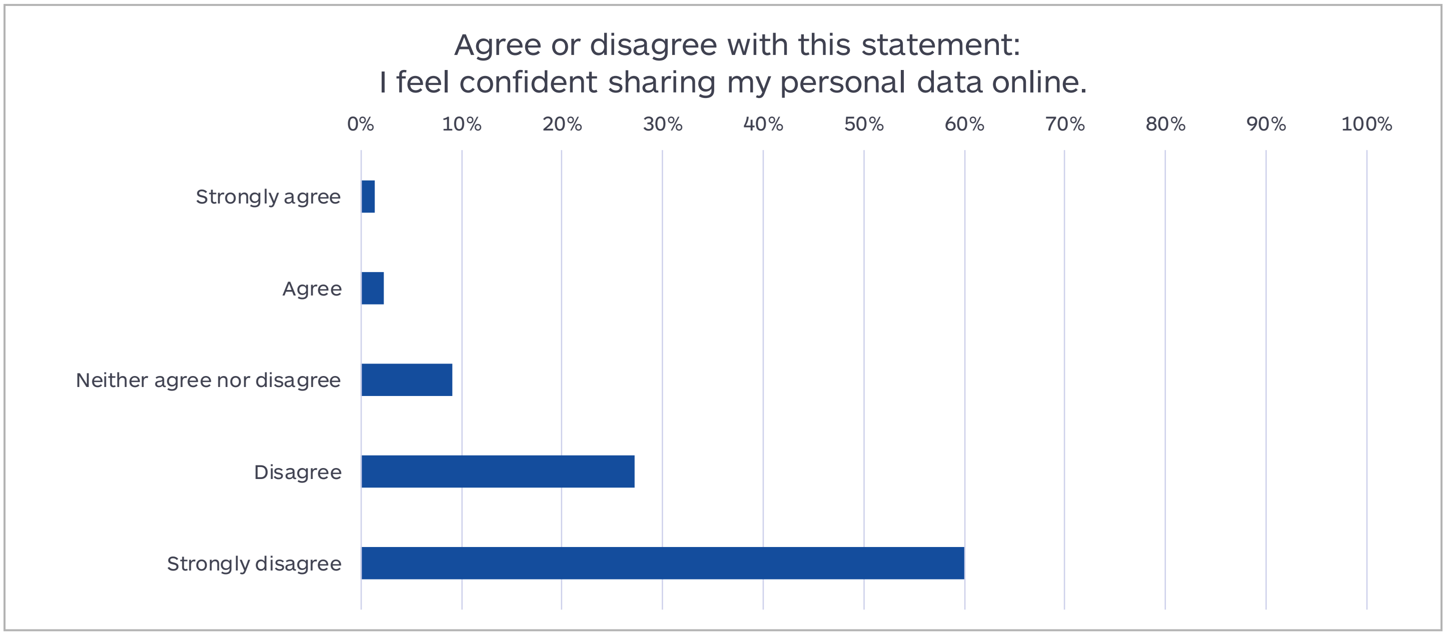

Figure 5. I feel confident about sharing my personal data online.

Most respondents strongly disagreed with sharing personal data online. In fact, most respondents (87 percent) are not confident about sharing their personal identifiable information online. Baby Boomers are the most conscious (almost 88 percent) when it comes to seeking data privacy at work and at home.

What data are users most likely to share? Respondents across generations who are confident in disclosing information are most likely to share their (1) contact details, (2) card details, and (3) banking and health-related data (with those specific sites).

However, numerous breaches over the last few years have shredded consumer confidence in data protection. Stolen data can and has been used for semi-targeted attacks, such as login credentials and personal information being used to craft convincing phishing emails.

While user confidence in protecting their own privacy is high, we find that users do not have confidence in social media's ability to protect personal data.

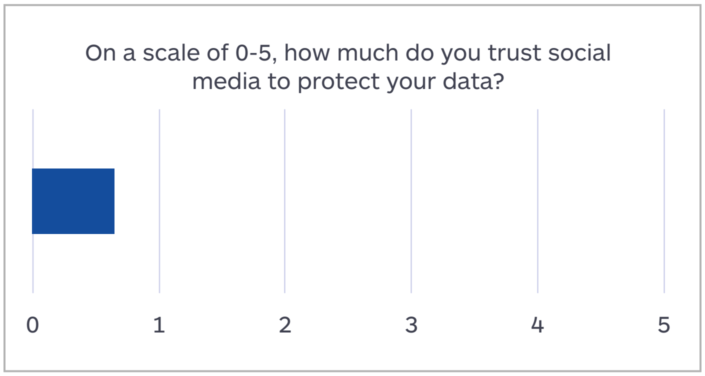

Figure 6. How much do you trust social media to protect your data?

We observed an average score of 0.6, out of 5, meaning that users barely trust social media, if at all, to protect their data. Baby Boomers are the most distrustful (96 percent) generation of social media when it comes to protecting their data, followed by Gen Xers (94 percent), Gen Z (93 percent), and Millennials (92 percent).

Users expressed a slightly higher degree of confidence in search engines' ability to protect data. While not high, the score at least surpasses that of social media.

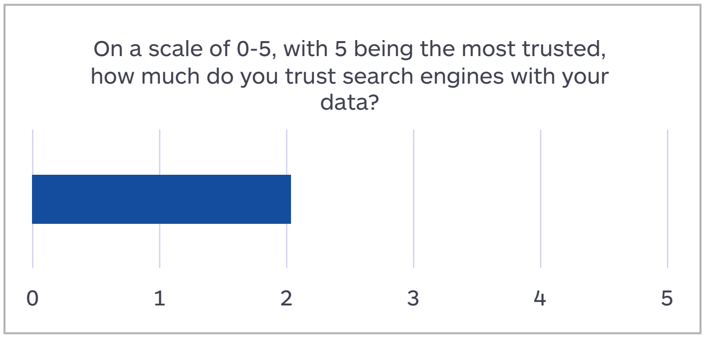

Figure 7. How much do you trust search engines with your data?

Among those polled, there's a common, healthy distrust toward social media and search engines, in general. Among the generations, not many Baby Boomers distrust search engines (57 percent) compared to Gen Xers (65 percent), Millennials (64 percent) and Gen Z (75 percent).

An overwhelming majority of all users (94 percent) refrain from sharing personal information on social media and 95 percent of polled users felt an overall sense of distrust for social media networks. If given the option to "choose the lesser evil," they'd rather forgo using social media than search engines.

Here is where the first comprehension gap comes into play, in the belief that search engine companies are more secure than social media. While the social media platform Facebook has been in the news for alleged phone call skimming and having the data of 50 million users stolen in a breach, search engine giant Google has been fined by the French privacy data protection agency for not disclosing what they do with user data in reference to targeted advertising.

A journalist for WIRED unsuccessfully attempted to keep the secret of their child's birth from the Internet, and learned that avoiding the eye of the Internet is almost impossible. It's an unfortunate truth that many of the privacy-invading policies that search engine and other online companies use are the same methods used by countless online companies to continue to provide free access to their content or continue their free services.

Facebook made money by selling ads, Google made money by pushing ads, and thanks to modern technology, more targeted and therefore successful advertisement campaigns are worth the extra overhead. In order to create these kinds of 'targeted' experiences for their advertising customers, organizations compiled "profiles" on their users, identifying their interests and shopping habits. This information is then used to send specific type of ads to those users, based on surfing and search history or likes and shares.

At the end of the day, in order to stay afloat and continue providing a service, if these companies are not going to charge their users for the access, they need to find the funds to keep their business running, elsewhere.

What we can do about it

Progress will not be stopped because of a lack of trust, and many developers have created tools to maximize privacy for those operating within the current constraints of the Internet's business model. Some privacy tools that users could embrace in order to avoid the great eye are:

» VPN: Virtual Private Networks provide a layer of anonymity by piping user data through a remote system.

» TOR: The Onion Router pipes a connection through multiple systems.

» Encrypted messengers: There are a few messaging apps out there that allow for full end-to-end encryption of data.

These three tools help keep a user from being tracked, profiled, or monitored. Unfortunately, just like with search engines and social media, there are issues with privacy software, not the least of which is a barrier to entry. If users don't read EULAs and change their passwords, will they take initiative to adopt VPNs, routers, and encrypted messengers? And even if they do, how foolproof are these tools for protecting users?

Virtual Private Networks

Not all Virtual Private Network providers are legitimate. In some cases, criminals will utilize hijacked systems as proxies and sell them as part of a VPN service. While connected to this criminal VPN, the criminal can easily collect user data.

Using a legitimate VPN that is known and trusted, regardless if it might not be "as anonymous" as a lesser known VPN is a good idea. Do some research before buying.

The Onion router

Users of TOR need to be worried about zero-day exploits for the TOR browser, and those that want to test the waters of underground crime should be aware of numerous stings performed by law enforcement over the years using TOR.

Therefore, the best option is to either avoid TOR entirely, or use it only at free Wi-Fi spots. Although keep in mind that sending any kind of personal data on an open network, or TOR, is not advised.

Messengers

Not all communication services are encrypted end-to-end and, in some cases, the government might be listening in on an encrypted chat, or at least trying to. Also, messengers are just as likely to be breached as other tools and services.

There are some popular end-to-end encrypted messaging apps out there, and some of them feel strongly about denying governments the ability to tap or circumvent their userbases' privacy. Once again, doing homework before selecting the correct messenger will go a long way.

Conclusion

It is easy to fall into the comfort of security hubris, of having faith that taking some action is enough to keep users protected. However, criminals and legitimate businesses alike already know these areas of weakness and will continue to exploit them. How long until users' distrust of social media and search engines turns into fear and action? How much more will we put on the user to stay protected until they finally crack?

Too many times over the past few years, we have seen examples of overly confident security teams having to deal with the fallout from a major breach, or users having to clean up the utter life-changing mess of identity theft. Want to know how many of the users who've been breached before are now skimming through EULAs? Our guess is very few. Don't wait until the proverbial stuff hits the fan. Take the extra second and think before you click. A good security plan should allow for flexibility, as no plan survives first contact with the enemy.

blog.malwarebytes.com corporate-sales@malwarebytes.com ☎ 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.