A guide to internet cookies and how you can control them

With the holidays right around the corner, many people are, like me, really looking forward to spending more time with family and friends. Another thing I'm looking forward to is the food we will be eating — specifically, the homemade cookies that are brought to these gatherings. A few can be a nice treat, but too many is always a bad thing for me.

The same can be said for the cookies that are dropped onto your computer or smartphone when you browse the internet. You will soon be flooded with different kinds of cookies, and there will be way more cookies than are good for you!

You know which cookies I'm talking about. That message that pops-up when you are browsing online asking you to "accept all cookies"? So, what do these internet cookies do?

What are cookies?

Cookies are little bits of code that a website will put in your web browser when you visit in order to keep track of what you do there and other information about you. They do all kinds of useful things – like remembering your preferences, what you put in your cart, or where you're located – so that your web browsing experience can be better. Cookies are also the primary way advertisers track your activities on the internet in order to show you more targeted ads and offers.

Are cookies good or bad?

In short, cookies allow companies and websites to identify a device and remember it then next time that they see it. This can be good or bad, as it depends on how that information is being used. Keep reading to learn the basics.

Types of internet cookies

Internet cookies can be delivered by all sorts of different people. Most websites leave several cookies on a visitor's device, but it's worth understanding the differences between different kinds of cookies. .

First-party cookies are delivered to your device by the website that you are visiting. These can be helpful as they are used to remember your preferences, such as displaying the site in English, and allow the site to offer you a more personalized experience. They can also remember what is in your cart which is great for holiday shopping.

Third-party cookies are those which are placed on your device by advertisers and are used to track your device after you have left that website and continue to follow you around the web. They allow the advertisers to serve you with personalized ads. Think about a time when you looked at a certain item, like a shirt, on a shopping website, but didn't buy it. Then you saw that shirt in an ad on your Facebook or Instagram feed. The cookies allow the advertisers to recognize your device when you visit other websites, and display their targeted ads. These cookies can persist on your device for over 30 days if you do not clear them yourself. Companies are starting to allow users to opt-out of third-party cookies, so advertisers are adapting to other tracking methods.

Another flavor of internet cookie is a session cookie. Session cookies are used when you log into a website by storing your login credentials every time you visit a particular site. Websites also use session cookies to improve site performance like fast page loads.

What kind of dangers can cookies pose?

If you’re a frequent internet user (and just about everyone is these days), it’s wise to understand the risks that cookies pose so that you can best determine when to delete them.

Privacy risk is the biggest concern for most people. It is typically not easy to discern exactly what data companies are collecting with cookies and who they are sharing that information with. Typically, advertisers and data brokers are the ones collecting information this way.

Another danger posed by cookies is cookie fraud. This involves the use of cookies to fake the identity of someone else to gain access to their account or use their identity to commit a crime. To reduce the risk of cookie fraud, it is important to avoid potentially malicious sites and keep your browser well protected by installing the latest updates when they become available.

Why do I see all those messages asking me to “Accept all cookies?”

Over the past couple of years, you may have noticed that a majority of websites have started to include a pop-up message asking you to allow them to place cookies on your device. This is done to comply with data privacy laws which were designed to protect users’ personal information and force companies to state what data is being collected and how it is being used.

The basic idea being these laws is that companies need to tell internet users that their data is being collected and if it is shared or sold to other companies, and that they should be able to say no. If it is a company that you trust or if you prefer a more personalized browsing experience, then you may prefer to accept cookies.

How to control your cookies

Now that we have a better understanding of cookies and how they are used, we can review the best methods for controlling cookies on your devices thereby allowing you to control your privacy more effectively.

For cookies that are already on your device, you can clear them yourself. In most internet browsers, within their settings you are able to manually clear your cookies or enable it so that cookies are cleared every time you close your browser. To prevent cookies from being placed on your device in the first place, you can sometimes opt out of third party cookies within your browser settings or decide what cookies you want to allow on a particular website by interacting with the cookie banner on the site. Certain cookies that are necessary to the site's performance will not allow you to opt out, but other types such as those used for advertising will allow you to opt out.

Many companies, including Avast, offer services aimed at helping individuals protect their privacy by preventing tracking. One of our solutions is a free browser-extension called Avast Online Security & Privacy that is available on all major browsers. It can block tracking cookies for you as well as other types of tracking online and is a great way to increase your online privacy at no cost.

DOWNLOAD FREE AVAST ONLINE SECURITY & PRIVACY

Keep in mind that by removing cookies you will encounter some inconvenience such as having to reenter certain information on websites since they will not remember you. On the plus side, you are less likely to feel like someone is following you online. As with the tasty cookies you may encounter this Holiday season, moderation is in your best interest, so keep those cookies under control.

Scammers love to take advantage of our altruistic tendencies — here's how to stay safe

The human impulse to help another human in need is one of our best instincts. But it's also one that attracts the worst of humanity. Unfortunately, scammers love to take advantage of our altruistic tendencies — and I recently received two messages online that highlighted just that.

The first message popped up in my Instagram DMs: "I need your help." Curious, I opened the app to find that a sustainable fashion brand I follow — not someone I know personally and not someone I'd ever spoken with before — had reached out.

Now, I had a feeling I knew where this was going — and I expect you do, too. But I decided to play along in order to see where they'd take it. And almost as soon as I responded "Hi, stranger on the internet!", the account replied with this:

"I was trying to login in to my new Instagram page on my new phone and they ask me to find someone to receive a help link for me, will you"

Still playing along, I asked, "Okay, so why would you need a stranger to do this for you?"

They responded with "Please," followed by the crying emoji and the praying hands emoji and this image:

...Which is not even a very good attempt at scamming? So I stopped playing along, reported the account, and posted to my own Stories about it.

Just a day later, someone I actually do know in real life messaged me on Facebook Messenger. This is a person I knew as a child, but who I haven't seen in 20 years. They asked, "Hey I really hate asking but can I barrow a few bucks until Wednesday?" To which I replied, "Hey friend! You get hacked?"

We kept talking and I could tell that, in this case, it really was my childhood friend. They were having a hard time financially and, I can only assume, were reaching out to whomever they thought might be able to spare some cash.

I chose not to lend them money, but wanted to share this story in order to illustrate how scammers use social engineering to trick well-meaning people out of money and/or personal information. Let's take a look at these two messages to highlight the obvious (and less obvious) red flags of scammin'.

Obvious scamming

The Instagram message I received is a good example of what I'd call "obvious scamming." As someone who spends a lot of time thinking about this stuff, I knew it was a scam pretty much immediately. But I'm not trying to gas myself up here. I honestly think most people would be able to spot this as a scam.

Here are the signs that anyone receiving a similar message should be aware of:

It's a person I've never actually spoken with.
They opened with a request: "I need your help."
There was an attempt at time pressure: "Please [crying emoji]"
The "screenshot from Instagram" that they sent me is rife with weird grammar and spacing.
There's no real situation where a person would need a total stranger to receive a link for them.

I took a look at their profile and they — a sustainable fashion company — were suddenly constantly posting about cryptocurrency.
So what were these (bad) scammers trying to achieve? I didn't continue with the ploy, so I can't say for sure. But I can make an educated guess, based on the fact that they wanted me to receive and click on a link for them.

Clicking on a malicious link can result in a couple of different outcomes: it could download a virus to your device; it could direct to you a site that asks you to enter personal or financial information; or it could be a link asking you to send money directly. In the case of my would-be scammer, I'd guess they wanted me to download malware, either to take my device by ransom or to gain access to my Instagram account.

Are they scamming?

The second message I received was a little bit trickier. Here are the red flags that it might have been a scam.

It's a person I haven't seen in 20 years, although they did randomly message me over Thanksgiving. They asked me (inappropriately, in my opinion) for money.
There was an attempt at time pressure: They told me they only had five dollars for the next four days.
Their grammar and spelling weren't great.
After just a couple questions, I was able to establish pretty quickly that they were who they said they were. One of the biggest signs was that they didn't keep pushing when I said I don't loan people money. A scammer is going to keep pushing and keep trying to find a way to convince you to do what they want. A real person might do that, too — but not pushing is a pretty good sign that you're dealing with the person you think you're dealing with.

This was also a pretty low-stakes situation. The relationship I have with this person is tenuous, at best: We've exchanged maybe 10 messages in the past 20 years, all of them in the past month or so. But a good scammer will use a much closer relationship to try to get money from their victims.

For example, "grandchild scams" are increasingly common. These scams target older people, with scammers posing as a grandchild who has gotten themselves into an urgent and dangerous situation. Sometimes they say they're stuck overseas after being robbed or maybe they claim to have been arrested. The "grandchild" begs the grandparent not to tell their parents, saying they'll get in trouble or they're embarrassed. Instead, they request that money be sent immediately.

In those situations, it's always important not to get swept up in the feeling of emergency. Grandparents need to call their kids to find out where their grandkids are, even if the "grandkid" they're talking to tells them not to. And never, ever send money — or gift cards or anything else that can be used like money — to someone who has reached out online.