The Hidden Danger of Unsubscribing from Emails

June 22, 2025 - Nobody likes junk mail. And with inboxes overflowing with spam, clicking that little "unsubscribe" link at the bottom of an email might feel like a quick fix.But think twice. Some "unsubscribe" links arenâ€™t safe. In fact, they could lead you straight into a trap. Hackers are now disguising phishing attacks and malware downloads behind fake unsubscribe buttons. These links might look legit, but clicking them could confirm your email address is active - or worse, open the door to identity theft.

What happens when you click? Best case? You just told a spammer that your email is real. Expect more spam. Worst case? You land on a fake website designed to steal your personal info - like your name, login credentials, or even your credit card.

In some cases, just clicking the link could start a malware download, infecting your device silently.

According to security firm DNSFilter, 1 in every 644 "unsubscribe" links is malicious. That may sound small, but with billions of emails sent every day, it's a real risk.

The reason these links are so dangerous is that clicking a link takes you out of the safety of your email app and into the wild west of the internet. On a shady site, hackers can use fake forms to trick you into entering your password or installing harmful software. Some even mimic the websites of big brands and well known companies.
There are safe ways to unsubscribe.

If you're tired of spam, use your email providerâ€™s unsubscribe button. In Gmail, look for a small blue â€œUnsubscribeâ€• link to the senderâ€™s address at the top. Apple Mail and Outlook offer similar built-in options.

You can also mark messages as spam. This trains your email to block similar messages in the future.
Block the sender is always simple and effective.

And finally, you can always setup filters to automatically send unwanted messages to the trash without ever seeing them.
Be careful with this one though, especially when using Gmail. Iâ€™ve personally found that using filters isnâ€™t always accurate especially if you have a lot of them. They can conflict with each other and Gmail wonâ€™t allow you to specifiy the order in which filters are executed, which can be very problematic.

If you want to see if your email has been compromised, take a look at HaveIBeenPwned.com. It will let you see if your email or passwords were exposed in past data breaches. If they were, change them ASAP and turn on two - factor authentication. The chances are that you will find your email address included. I have several addresses that I use and every one of them, including my address here at ACCESS, had been included in at least one data breach.

The bottome line here is that if youâ€™re not sure who the sender is, donâ€™t click anything. When it comes to email, curiosity doesnâ€™t just kill the cat - it might cost you your identity.
Rule of thumb:
If an email smells fishy, treat it like phishing.

by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here.
Registration is easy and free.

Follow ACCESS