



# NEWSLETTER



## Is Your Inbox Drowning in Spam? Here's Why (and How to Stop it)

If you've been swamped with spam lately, you're not alone. Unwanted marketing messages clogging up our inboxes seem to be part of everyday digital life. But have you ever stopped to wonder how on earth all those spammers acquired your email address?

### Entering Online Promotions and Contests

As annoying as it is, there are a few common ways that marketers legitimately come into possession of our contact info. One is when we enter online promotions and contests, those tempting offers we've all seen for things such as cars, vacations, and gift cards. On the surface, they seem like a fun chance to win a prize, but before you enter, it pays to read the fine print.

You'll usually find terms stating the company reserves the right to share or trade your email address with affiliates and other third parties. So, by hoping for that dream vacation, you've given permission for your info to be sold to the highest bidder.

### Publicly Displaying Your Email Address

Another invitation for spammers is posting your email publicly on social media profiles, personal blogs, forums, comments sections, and more. Savvy bot programs are constantly prowling the internet, collecting any unprotected contact info they find displayed online. Worse still, some people foolishly use their primary personal email as their public username on major sites such as Facebook or Twitter. This tells spammers exactly who you are and provides them with an all-access pass straight to your inbox.

### The Impact of Data Breaches

No company or individual is immune from the threat of data breaches either. When a huge repository of private user records is stolen, such as in the infamous breaches of LinkedIn, Yahoo, and Marriott, cybercriminals are offered a massive, gift-wrapped list of potential spam targets all in one place. Check [HaveIBeenPwned.com](https://haveibeenpwned.com) regularly to see if any of your online accounts were unintentionally caught up in one of these digital heists.

### Engaging With Spam Messages

Astoundingly, even avoiding and deleting suspicious messages isn't always enough to escape notice. Advanced tracking allows spammers to monitor whether an email address actively opens or engages with a particular promotional email in any way. Unfortunately, clicking unsubscribe links achieves the opposite goal by verifying the account is live and operational. Interacting at all, even to get rid of the spam, teaches marketers your inbox is ripe for more bombardment.

### Prevention and Protection

Once out, that contact info genie doesn't want to get back in the bottle so easily. The best prevention tactics involve limiting what information you display online. Top-tier spam filters and security programs are also crucial defense layers against the onslaught.

### When All Else Fails

If you've exhausted other options and spam continues plaguing your inbox, let our technicians handle it from here. We can install robust commercial antispam software tailored to your specific email usage.



## The Convenience and Risks of QR Codes

### QR Codes Go Mainstream

Quick Response (QR) codes have been around for over 20 years, but it wasn't until the COVID-19 pandemic that they truly broke into the mainstream. As businesses needed safe, contactless solutions, QR codes provided an easy way for customers to access menus, place orders, log into WiFi and more – all without touching shared surfaces.

Their growing adoption has undoubtedly brought many convenient new features to our daily lives. But as with any new technology, QR codes also introduce some cybersecurity risks people should know. In this article, we'll explore common QR code threats and tips for staying safe.

### How Hackers Can 'Qish' QR Codes

By their nature, QR codes aren't human-readable – they're just patterns that direct your device to a website or app. This is what also makes them vulnerable to exploitation. Hackers have figured out simple ways to replace legitimate QR codes with fraudulent ones.

You may have noticed how many restaurants now offer digital menus through codes posted on tables. But what if an attacker replaced that code

to route you to a clone website instead?

You may not realize you've been redirected from the actual restaurant site without closer inspection. And if you enter payment details on the fake page, hackers now have your sensitive financial information.

The same risk applies to QR codes in public spaces promising things like free WiFi or rewards. An imposter code could install malware on your device or phish your login credentials once you connect.

The security industry calls this type of QR code fraud "Qishing" – the QR equivalent of phishing scams.

### How to use QR Codes Safely

To mitigate risks, follow these basic precautions when scanning any QR codes:

- Inspect codes for signs they may have been tampered with, like extra stickers or font/format mismatches from the business's usual branding.
- Verify the destination URL and ensure it matches what you

expect from the legitimate organization.

- Think twice before entering passwords or payments via public codes.
- When in doubt, type the business URL directly or visit their official website first before interacting with any embedded QR links.

With a bit of mindfulness about QR code sources and where they lead, customers can continue enjoying stress-free conveniences while minimizing the chances of running into fraudulent scams and clones.