Can You Get a Virus Just by Opening an Email?

Is it possible to get a computer virus by simply opening an email? It's true that email has been and remains one of the most popular attack vectors. Hackers, spammers, phishers and scammers are all knocking on the door of your inbox. But how easily can they slip in, and wreak havoc on your computer? Let's find out...

Viruses and Other Threats in Your Email

The probability that you could be infected by an email-delivered virus just by opening a message was once terrifyingly large. But the vulnerabilities that made it so were quickly addressed by developers of email clients and antivirus software. Today, you have to do some pretty foolish things to catch a virus via your email inbox.

But myths, urban legends and endlessly repeated tales of the cousin of the friend of a friend who lives near the police station in a major city, who got a virus by opening an email, those die hard on the Internet. And ironically, these tales live on and are propagated largely by email. You may still get warnings about the Hallmark Virus, and similar missives warning you not to open emails with certain subject lines, or a horrible uncurable virus will wipe out your hard drive.

The possibility of virus-infected email arose with the introduction of HTML email, way back in the early 2000s. HTML gave us the ability to use fonts, colors, images and fancy formatting in emails, but it could also contain hidden executable code in the form of Java or Javascript. That code could do the bidding of bad guys if it could be triggered to execute. Opening an infected HTML email, or even allowing your email client to display it in the preview pane, could execute the code.

The good news is this vulnerability was noticed almost immediately, and steps were taken to close it. Email clients stopped supporting Java and Javascript. Vulnerabilities in email software and operating systems were patched. Spam filters began blocking emails that contained suspicious code. Email-scanning was added to anti-malware programs.

Some people don’t send or read HTML; they stick with old-school plain text email. That’s a sure way to avoid triggering embedded malicious code, but it makes for a poor email experience. Also, it doesn’t entirely protect against email-born malware.

Beyond the First Click: Other Email Threats

The likelihood of being infected just by clicking to open a message sitting in your inbox is vanishingly small. It's zero if you allow Windows to automatically update, and you have anti-virus protection. But once you open that email, other dangers lurk. **It's the second click that'll get you in trouble.**

Files attached to either plain-text or HTML email can contain viruses. That is why it is so important not to click on any attachment whose sender you do not know and trust. **Even if you do know and trust the sender, caution is needed.** The email sender's address can be faked, or the sender's computer may have been compromised, so it’s vital to use anti-malware software that scans every email attachment. (Right-click on the sender’s email address, then click on properties. The id of the actual sender will appear. If it is different, it’s a bogus! Back off and immediately delete the email!

The bad guys out there rely mainly on social engineering to entrap victims these days. Typically, that means a phishing email that masquerades as something from a trusted sender, urging you to click on a link in the email. Some typical ploys often try to pique your curiosity by mentioning celebrities, public figures or current events. Have you heard? Willie Nelson Confirms Unfortunate News!

Other emails may pretend to be from a company that you know, such as your bank, Paypal or eBay. Oh no... your account is about to be suspended! One false click and you could be dealing with a nasty virus or caught in the snare of identity thieves.

One of the things that many people like about web-based email, and GMail in particular, is that you're protected from most of these threats without installing any software at all. If a message with a suspicious link or attachment comes your way, it's either blocked completely, or a warning is displayed that the content may be malicious. It’s not unusual for a GMail spam folder to catch dozens of bogus messages every day.

If you use webmail, or you're conscientious about keeping your desktop email software up to date, there is no reason to fear that you will catch a virus simply by reading an email. But be careful about clicking on links or attachments. That's where the trouble starts.