How To Keep Your Email Secure From Hackers

Written by Devin Wise

Every day, the world sends around 205 billion emails. Of course, most of them are inconsequential: recipes and poems about horses that grandma forwards to everyone on her contact list. Yet every day, billions of emails are also sent that contain sensitive information. There's a good chance that in the past week or two, you've sent an email or two in your work life or your personal life (or both) that you wouldn't want somebody snooping on.

So how easy is it to hack into somebody else's email? In an age when even high-ranking officials have seen their email compromised repeatedly, that's a question that weighs on a lot of people's minds.

How Easy Is It to Hack Email?

The short answer, of course, is: "It depends." But how easy is it to hack your email? Probably easier than you think. In fact, a 2011 study found that it with the help of an online tutorial, regular people with no technical background were hacking each other's emails using a man-in-the-middle attack within just 15 minutes.

Broadly speaking, there are three ways a hacker can get into your email:

1. The hacker penetrates a security flaw within your email system that gives them access to your messages.
2. The hacker gets into your account directly by guessing or brute-forcing your password. This ranges from easy to virtually impossible depending on how complex your email password is.
3. The hacker tricks you into voluntarily providing login information somehow (perhaps phishing via a fake login page designed to look like your email, perhaps via malware the hacker got you to download or run on your computer somehow). One common approach is to get the user to install a keylogger, which then silently records every keystroke they make, allowing the hacker to search the records for the user's email login, which will typically be immediately followed by their password.

The first type of hack—finding and exploiting a flaw in your email system—is possible, but difficult. Unless you're using a privately-constructed email server (in which case only you know how secure your system might be), chances are you're using a publicly-available email service like Gmail. These services are massive, and because hackers are trying to crack into them all the time, Google employs hundreds of people to ensure that that doesn't happen. That's not to say that it doesn't, of course. In fact, a bunch of major mail services had millions of their customers hacked earlier this year, although it's not clear whether the hacker took advantage of systemic flaws or used some other approach to get in.

But the relatively good news is that because hacking into a system by finding and capitalizing on a security flaw is time-consuming, difficult and risky, the chances of an "average Joe" (or even an average Joe company) being the main target of such an attack are relatively slim. Unless you're famously wealthy or your email is full of tantalizing secrets hackers would know about, it's unlikely that you would be targeted

specifically by this type of hack. That said, your data could still be compromised if the email service you use gets hacked and user data is posted online or sold en masse.

The second and third types of hacks are significantly easier. While constructing a sophisticated phishing operation requires time and technical skill, virtually anyone with a few minutes to read a tutorial or two and download some software could try brute-forcing your account or installing a keylogger on your machine, especially if they have physical access to it. Keyloggers can also be installed and operated remotely, but this is more technically difficult and generally would require tricking you into downloading some malware.

How to Secure Your Email as an Individual

If you're using a third-party service, you may not be able to completely prevent email hacks, but there are a lot of things you can do to minimize the risk (and minimize the damage if your account is compromised somehow).

- Use a secure, unique password. This is a no-brainer, but the reason you hear it all the time is that many people still don't do it. Yes, there are even folks out there—probably thousands of them—whose email password is "password." Using too simple a password or using the same password you use on other sites greatly increases the chances of your email being compromised.
- Use encryption software for sensitive emails. Compared to just booting up your Gmail, setting up email encryption software (and ensuring your recipient has the ability to read your encrypted message) can be quite a pain. But it's certainly less of a pain than getting hacked, and once you get your encryption system set up it becomes quite simple to use. There are tons of options out there when it comes to email encryption software, so if you shop around a bit, you can almost certainly find something that fits well into your existing workflows.
- Restrict physical access to your machines. If a potential hacker can physically access your machine (to install a keylogger, for example), hacking your email becomes child's play. Use a secure, unique password on any system that you use outside of your home, and be sure to log out whenever you're stepping away from the screen.
- Avoid public WiFi connections. Remember those folks who learned to crack email using man-in-the-middle attacks in just 15 minutes? That's the sort of thing that can be very easy to do on a public WiFi network; the hacker simply snoops on all the information that's getting sent through the network and collects your account details and passwords in near-real-time as you use them. Using a VPN or some other form of encrypted connection is best if you must connect to public WiFi, but the safest approach is simply to avoid it entirely.
- Don't click sketchy links. This seems like another no-brainer, but a lot of email hacks happen because the user downloaded malware that installed a keylogger, or clicked on a phishing link and entered their account info into a hacker's fake website. Be very careful, as hackers can spoof emails that look like they're coming from your friends or from some authoritative source such as Google. If you're not sure, ask before you click. When in doubt, always err on the side of caution.

How to Secure Your Company's Email

If you're in charge of your corporate email server (or know someone in IT you can talk to), there are few more things you can do to help ensure it remains un-hacked.

- Educate employees. Remember, the weakest link in any security system is humans. Even the best email security isn't going to stop much if your workers are constantly falling for phishing scams and downloading trojans. So be sure that everyone at your company is on the same page when it comes to email. And be sure that emails containing sensitive company data are always sent encrypted rather than in plaintext!
- Encrypt your server connections. Don't stop encryption at email messages; it's safer to also encrypt your server connections using Transport Layer Security (TLS). Chances are whatever server system you're using already includes TLS options, but they may not be enabled by default.
- Verify senders. One of the best ways to stop phishers is to be able to spot and weed out spoofing/phishing emails before they ever reach their targets. Activating reverse DNS to find and block spoofing senders is a good idea, as is installing software that allows employees to sign encrypted emails with a verifiable digital signature so that the sender's identity is always clear.
- Keep your system's software updated. This is another no-brainer, but (again) one that people regularly ignore. Keeping your systems updated will ensure that when known security flaws get patched, your system gets patched too. If you're running old software, chances are it has at least a few known issues that a skilled hacker might be able to exploit.
- Scan emails for questionable content. Not all companies may be comfortable with this, as scanning employee emails is a form of snooping in its own right. Yet scanning incoming emails can help you block messages that look sketchy (phishing emails may contain similarities and phrases that a computer system could learn to detect and block automatically). Scanning outgoing mail for sensitive company information could help you ensure that employees aren't sending any data to people they shouldn't be.

Ultimately, there's no way you can totally secure your email. But armed with the above information, you should be able to make hacking your email a heck of a lot harder, and significantly reduce your own risk of becoming a hacking victim.