7 Alarming Things a Hacker Can Do When They Have Your Email Address

Send emails from your address

This is probably the most obvious thing hackers can do with your email address, and it's a nuisance for sure. Once hackers have your email address, they can use it to target more than just you, sending out email blasts to anyone (maybe even everyone!) in your contact list. As Garry Brownrigg, CEO & Founder of QuickSilk, explains, "They can 'spoof' an email message with a forged sender address—they don't even need your password for this." The things they send can be anything from harmful malware to scams and requests for money; either way, you'd certainly rather they didn't come from your address. And though it's mostly harmless (most savvy Internet users are able to catch on when they receive a scam email from a friend's address), it could still be a problem in some cases. "If a criminal really wanted to hurt someone, they could use this as a way to catfish a romantic partner, hack the victim's employer, get the person in trouble at work, or cause any number of problems in their personal or professional life by impersonating them online," says Jason Glassberg, co-founder of Casaba Security and former cybersecurity executive at Ernst & Young and Lehman Brothers.

Send phishing emails

Since there isn't a ton that hackers can do with just the email address, they're not going to stop there. "When a hacker knows your email address, they have half of your confidential information—all they need now is the password," warns Greg Kelley of Vestige Digital Investigations. They employ a few different methods to access it, the most common being the phishing email. This is an email, in the guise of being a legitimate email from a trusted source, designed to trick you into logging in. "They might create a legitimate-sounding email that appears to be sent from a service such as Amazon, eBay, Paypal, or any number of other popular services... Links in phishing emails will always direct the user to a purposefully built website that looks identical to the real service," explains Ray Walsh, a digital privacy expert at ProPrivacy.com. "However, if people use the login on that fake website, the hacker instantly receives the credential and password for the real account." Another way they can do this, ironically, is by sending you an email saying that your account is compromised or has been accessed from a new device, so you need to change your password for security reasons. (You've almost definitely gotten one of those at one point or another!) When you change your password, then your account really *is* compromised and the hacker has your password. Once hackers have your password, the range of things they can do becomes much greater. Luckily, being able to recognize these signs you're about to fall for a phishing email can keep you from falling victim.

Access your online accounts

Nowadays, our emails do double duty as our logins for scores of social media sites, in addition to Google Docs, online retailers, and so on and so forth. Internet users also have a very understandable tendency to use the same passwords for all of these accounts. And even if you don't use the same password, the hacker can click the old "forgot password" button and use the resulting email—which comes to your email address, which they *do* have the password for—to change the password, and voilà. Your accounts are their accounts, and they have access to anything on them that you do.

Access personal information

These things hackers can do with your information seem to be something of a chain reaction. Once a hacker has access to your online accounts, just think about all of the information that can then be right at their fingertips. Allan Buxton, Director of Forensics at SecureForensics, sums it up: "At a minimum, a search on Facebook can get a public name and, unless privacy protections are in place, the names of friends and possibly pictures," he says. "Throw that email address into LinkedIn, and they'll know where you work, who your colleagues are, your responsibilities, plus everywhere you worked or went to school previously. That's more than enough to start some...real-world stalking. That's just two sites—we haven't talked about political views, travel, or favorite places they might glean from Twitter, Foursquare, or Instagram." Glassberg admits that such "real-world stalking" is rare, sure, but anything is possible in an era where people document nearly everything online. This is part of the reason that there are some things you should never, ever post on social media.

Steal financial information

Things start to get really problematic if hackers are able to find your credit or debit card information—which, more likely than not, you've sent via email at one point or another. Your online bank accounts can also be a major target for hackers, especially if you use your email address as a login for those, too. And, needless to say, once a hacker has access to those, your money is in serious jeopardy. "This is one of the biggest risks you'll face from an email hack," Glassberg says. "Once [hackers] have the email, it's easy to reset the bank account and begin issuing transactions." In addition to potentially being devastating to your finances, this can also hurt your credit score, as BeenVerified's Chief Communications Officer Justin Lavelle explains: "Cybercriminals can use your credit card details, open bank accounts in your name, and take out loans. It will likely ruin your credit card’s rating and your credit report will take a hit."

Blackmail you

As if things weren't scary enough, hackers can use your personal info to ruin, or threaten to ruin, your reputation. This is fairly rare, but it can happen, especially if a hacker finds something that the user wouldn't want to be seen publicly. "[Hackers] can use this access to spy on you and review your most personal emails," says Daniel Smith, head of security research at Radware. "This kind of information could easily be used to blackmail/extort the victim." These red flags someone might be spying on your computer can help you stay ahead of a scary invasion of privacy like this.

Steal your identity

This is definitely a worst-case scenario, but "once the hacker has your personally identifiable information, they can steal your identity!" Brownrigg warns. With information like your social security number and credit card info, identity theft can sadly be well within reach for hackers. So if you start noticing these signs someone just stole your identity, consider that your email address may have been compromised.

How you can stay safe from hackers

Hopefully, though, you won't have to encounter any of these problems, and there are some measures you can take to keep your information safe. Avoid using your verbatim email address as a login for other sites, and make sure that your password is strong and difficult to guess—check out our guide here for creating a strong password. You should also change those passwords every couple of months or so for maximum security. Glassberg also recommends securing your email account with two-factor authentication. This "[requires] a one-time code to be entered alongside the password in order to gain access to the email account," he told RD. "In most cases, the code will be texted to the person's cell phone, but there are also 2FA apps you can use, like Google Authenticator." And, of course, just use your common sense. Don't share information or type in your email password on public WiFi networks, and just be smart about the information you share over email.

What to do if you think you've been hacked

Starting to notice some strange online activity? There are a couple of ways you can try to get ahead of it before it gets too bad. If you hear about spam emails being sent from your address, change your password immediately. You should also tell your contacts so that they know to ignore anything coming from you. Finally, Lavelle offers some other suggestions: "Change your email settings to the highest privacy setting, scan your computer for malware and viruses, and be sure your browsers are updated," he says. And you can also stay ahead of hackers by learning the cybersecurity secrets hackers don't want you to know.