How Spammers Spoof Your Email Address as the Sender

It's maddening when your email inbox gets a fresh load of spam dumped on it. Equally frustrating is when spammers spoof YOUR address as the sender, and all your friends start asking why YOU are sending them unwanted sales pitches for dubious products. Understanding how spammers get your email address can help to prevent both of these problems. Here's how spammers get your email addresses, and steps you can take to protect your inbox...

Is Your Email Address Vulnerable to Spammers?

The bad guys harvest email addresses by pretty mundane means. YOU may even be contributing to the problem without realizing it.

Using web-crawling "spider" programs similar to your search engine to index Web pages, some spammers hunt down email addresses by looking for the telltale "@" symbol. Spiders can harvest millions of email addresses automatically. To avoid being "bitten" by an email harvesting spider, don't put your email address on public spaces on the Web. *That means not posting it to online forums or personal web pages*.

Do a Google/Edge search to see where your email address is available, and work towards becoming invisible. *(Tip: enter your email address in the Google/Edge search box enclosed in double quotes.)* If you must make your email address visible in public, you can obscure your address by avoiding the "@" symbol, i.e., use "bill at cox dot com" instead, create an image with the address, or use a disposable email address.

"Dictionary attacks" are another way to collect email addresses. This method, which combines common words with popular domain names, relies on the fact that you don’t need a valid email address to generate an outgoing email. Spammers generate emails to computer-generated addresses, accepting millions of bounce-backs in exchange for a handful of replies from valid addresses. That's why the first rule of dealing with spam is "don't reply to it." Doing so just tells the spammer that you are a "live one" and worth hitting with more spam. Delete that unwanted message, or banish it to the Trash folder.

You can make it harder for a dictionary attacker to guess your address by NOT choosing any combination of dictionary words, common first or last names, and a string of numbers. If your email address is smith123@aol.com or susie90210@gmail.com, you'll get loads of spam, no matter how careful you are. Those addresses are just easy targets, because they're so easy to guess.

Many people simply hand over their email addresses, no questions asked, just to get access to a game, contest, some free program, a ringtone, or other valuable prize. It's a good idea to have a "throwaway" email address that you can enter into Web forms, rather than using your everyday address.

If you have an email password that's easily guessable, someone may hack into the email account and steal all of the contacts stored there. If your computer is not adequately protected from viruses, spyware and phishing attacks, all of the people in your email address book are vulnerable to spam attacks as well.

Email "forwards" play into the hands of spammers, because they accumulate a large number of addresses as the message spreads from one person to another. If even one of those recipients had their email hacked (or computer compromised by malware), the entire trove of addresses would be vulnerable.

Data Breaches: An Ongoing Privacy Menace

Hacking into a major company's databases can yield millions of high-quality email addresses at once, not to mention even more valuable data such as credit card numbers, Social Security Numbers, etc. In December 2016, Yahoo confessed that over one BILLION of its users' accounts had been hacked three years prior. Target, Chase Bank, American Express, Home Depot, Apple, Sony and other large companies have reported hacks in recent years, resulting in many millions of accounts being compromised. (Now, think MGM!)

The Big Kahuna of Data Breaches was reported in September 2017. The Equifax hack was especially damaging, because it revealed names, addresses, Social Security Numbers, birth dates, driver's license data, credit card numbers, and email addresses. Since then, high-profile data breaches revealing untold millions of customer records have become a common occurrence. By combining all of that data, Bad Guys can create much more sophisticated and compelling email scams.

Spammers also trade in lists of email addresses. A list of a million addresses gleaned from a data breach might go for as little as $100. Some online crooks don't even mail spam, but make their living harvesting and trading email addresses.

Before signing up to any mailing list, make sure you know what the email privacy policy is. Opt out of allowing your email address to be shared with third parties for any reason, if possible.

The fewer entities that have your email address, the less spam you will receive. Think before you give your email address to any website. Using a disposable email address, keeping your own computer secured, and encouraging your friends and family to do likewise will also help.