By Jen Sharp, jensharp.com

Can You Prevent Your Email Address From Being Used by Spammers?

BAD NEWS

It seems like a normal busy day with your regular slate of tasks ahead of you. Then a strange email comes into your inbox. But you're used to spam. Then another. And another. Suddenly, a thousand emails later, you are stuck. Another victim of email spoofing.

Whether or not this has happened to you, questions abound:

"Am I being hacked? What data is compromised? Why do people do this kind of thing? Should I even worry about it if it hasn't happened yet? What could I do if it does happen?"

While consistent solutions are still emerging in the industry, here are a few answers.

"Am I being hacked? What data is compromised?"

Hacked. Spoofed. There is a difference. Chances are, your email address is being spoofed, not hacked. Spoofing occurs when a person of questionable intentions finds your email address somewhere. It could be found from your website using a "robot" of sorts that searches for words formatted like an email address. Or it could have been randomly generated just from your domain name. Or it could be listed anywhere and picked up manually. The email thief is only borrowing the name of your email address, not your email service. Using easy tools, anyone can compose an email and make it look like it came from a different email address. The spammer would not have to get into your computer to be able to simply use your address as a front for sending out phishing or spamming emails. The deluge of emails you get would normally be in the form of rejected or bounced emails telling you that the recipient did not exist. Spoofing is very easy to do and requires only an email address.

If you suspect instead that you have been hacked, the easiest way to tell is by checking your "sent" mail or outgoing mailbox.

If you suspect instead that you have been hacked, the easiest way to tell is by checking your "sent" mail or outgoing mailbox. If you see that those emails in fact originated from your email client and service, then you have been hacked instead of spoofed. (That is another article itself, but at least change your passwords!) If none of the spamming emails are in your sent mail, it is just spoofing and no system or login breach occurred.

"Why do people do this kind of thing?"

We are all used to spam by now. Filters and email providers cannot block all of the unwanted emails. We have become fairly good at seeing an email address that isn't familiar accompanied with a strange subject line or attachment, and just deleting it or sending it to Spam folders without batting an eye. Spammers want you to open their emails. If someone you know who trusts you receives an email from you, they are likely to open it without checking. That is why they want to cloak their real email in your good email address. When end users click to open mail, some clients may automatically open pieces of the mail that could contain and extract and install malware or adware. Or, if the email looks professional enough, it could contain a link asking for sensitive data or login verification. That’s phishing, and unfortunately, it fools many people.

“Should I even worry about it if it hasn’t happened yet?”

Anyone using a Gmail, Yahoo, or Hotmail email address is very susceptible to being spoofed due to the popularity of these free services. If a spammer wanted to know if a certain address was in use and available for spoofing, all they would have to do was try to sign up for an account, get the message that the address was unavailable, and use that for a front. It’s likely that you will be spoofed at some point, so you might think about taking steps to protect your address.

Any water district, city or even business that has their own domain name usually has email addresses using the domain. This is a very professional way to conduct business and serve customers and is recommended highly, but it comes with the susceptibility of being spoofed. A spammer can find an email associated with your domain, use it to spam, and your cluttered inbox is only the first of your problems. Email service providers may blacklist your domain, moving all emails from your domain name into spam folders as a service to its customers. As a result, your constituents may have your legitimate emails blocked.

“What could I do if it does happen?”

If you have ever been spoofed, you know that eventually spoofers will be tracked by IP and shut down, then move on to another email address. You simply have to wait it out in most cases. In severe cases, you can call your email provider and see if the spamming is bottlenecking the mail server with requests stacked up ready to send, and suggest that they restart it. That will delete the mail not yet sent through the server, fortunately including all the spam, but unfortunately including legitimate emails. They may or may not be willing to do this, but it would be worth asking in severe cases.

Prevention is better than reaction.

Prevention is better than reaction. There are a few steps you can take that may make you less of a target for spoofers:

- First, avoid using popular free email providers addresses. While you may use their services, a customized email address using your domain name is more professional and controllable.
- Second, you can prevent your email address from being picked up from your website by enclosing its script or by directing emails through a contact form instead.
- Finally, you can ask your email service provider what options they offer for email authentication.

For example, emerging as solutions are SPF (no, not sunscreen protection factor)… Sender Policy Framework, and DMARC… Domain-based Message Authentication, Reporting & Conformance. If you have a domain that has emails associated with it, this solution may work for you, and most providers will implement it free of charge. If a mail server receives an email, it checks to see if the sender is valid according to that domain. Unfortunately right now, frequently one recipient server is performing one set of checks, while a different receiving server makes another set of checks or treats the messages that fail in a completely different way. For example, Gmail allows emails that failed the check to come through. Outlook does not. Exchange lets everything in while OS X accepts but flags failed checks as spam. Google Apps for a domain and GoDaddy domains work well in connection with these checks, but the sender and recipient must also have the same system of checks for it to be effective. These systems can be put in “monitor mode” first to ascertain that legitimate emails are not being sent away. After some time gathering feedback, they can be put in “reject mode.”

While there may be no such thing as SPOOF PROOF, there are some simple steps you can take that may protect you from being a target.

Since 1997, Jen Sharp (JenSharp.com) has served business and government across Kansas and the US and even internationally, specializing in Web development, design & programming including e-Learning, ecommerce, content management systems, and other small business solutions.