By Carl Brown, President, GettingGreatRates.com

Twenty-five thousand emails in my inbox. All but 25 of them had subject lines like, “Sending Failure” and “Message Rejected.” I was spoofed. It was awful. But my story might help you avoid being spoofed, too.

December 17, 2015: Four hundred email failure messages. “Hmm,” I thought. I should have thought deeper!

December 18: Four thousand failure messages. I won’t say what I thought.

December 19: Twenty-five thousand failure messages, give or take a few thousand. What WAS I thinking?

> Email spoofing is the creation of email messages with a forged sender address. – Wikipedia
> (Spoofing is done to send out junk e-mail, phishing e-mail or just to be malicious. – The Author)

Finally, I took action. I killed my email address, my identity for the last ten years – ouch. Later on I discovered killing an email address won’t stop spoofing. Thus, began my research into spoofing. Amazingly, there is not much guidance out there. This is what I picked up.

You prevent and stop spoofing by doing the same things:

- If you use Gmail, Hotmail or another on-line service, they should already have spoof prevention in place but don’t just assume they do. Call tech support of the host of the server that carries your email to make sure that the next bullet point measure has been activated for your email account.
- If your city or district has a Web site and you run email through that site, you are vulnerable. Call tech support at the company that hosts your Web site. Tell them you were spoofed, or you want to prevent spoofing (hopefully the latter).
  - ❖ Under the guidance of tech support, go to your Web site settings page.
  - ❖ Open the “DNS Zone File” page and set the “TXT Record” value, which exerts control over email, so that email with your address on it will only be claimed as yours if it actually came from your host’s server. The thing that does this is called a “SPF Record.” The SPF Record tells other people’s email servers that if they get an email with your address on it but it came from any other server, REJECT IT.

Now, you can actually set the SPF Record so that it will allow your email to be sent from other specified servers, too, but that is way above my pay-grade.

Spoof and spam prevention – related – are really the way to go:

- Protect your usernames and passwords, make them complicated and change them often – old but excellent advice.
  - ❖ Do you have too many usernames and passwords to remember? Record them. But don’t put them on your Web-accessible computer or other device! If

> Spoofers are like a pack of hyenas. When they sense injury they all jump on. Soon after that, those who received spam and phishing e-mails under your name start to call and e-mail YOU. And you learn some new bad words.

Domain Name System (DNS) File is a text file that describes a DNS zone. The zone file contains mappings between domain names and IP addresses and other resources, organized in the form of text representations of resource records (RR). – Wikipedia

someone gets in or steals the machine, game over! If you don't have many passwords, write them down and hide the list well in two separate places – your office or home and a safe deposit box or maybe at your Mom's house. If you have a lot, put them on two flash drives and hide those in two places, one nearby, and one at Mom's house. Continuously update the one that you keep handy and periodically change it out with the one at Mom's house. (Morose, but important, that flash drive is going to come in handy for your loved ones when you die.)

TXT (Text) Record is a type of resource record in the Domain Name System (DNS) used to provide the ability to associate some arbitrary and unformatted text with a host or other name. – *Wikipedia*

  - If you (still?) trust the Web, use one of those online password lockbox services. I, for one, do NOT put the keys to my life on the Web. I hide them in a safe, physical place.
- Be careful about email addresses on your Web site. Spammers, spoofers and "bots" can find them there and abuse them. Do this:
  - Hide email addresses behind a contact page that has an authentication feature. You know, a page with a fuzzy picture of numbers or a word that you type into a box to gain access. Bots can't (yet) read those fuzzy things. Sure, it's not user-friendly but it's effective. Or,

Sender Policy Framework (SPF) Record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain. The purpose of an SPF record is to prevent spammers from sending messages with forged "From" addresses at your domain. – *Google*

  - On your contact page, tell readers how to build email addresses from a list of names and addresses you give them. And/or,
  - List a "disposable" email address like info@yoursite.com. Whoever receives these messages then forwards each to the proper staff for handling. When you start getting too much spam at the disposable address, just delete it and start a new one.
- When you set up an online account and they offer two-stage verification, take it! Two stage is a login process where you enter your username and password. The site then sends a text message to your cell phone with a code. You enter the code into an authentication box and you are in. To get into your account a thief would have to steal your username, password and your phone. Please don't say you put all that information in your phone!
- Install a SSL Certificate on your Web site. This encrypts contact between your site and others who visit your site, making it much harder for someone to hack your visitors' information.

Secure Sockets Layer (SSL) Certificate creates an encrypted connection between your web server and your visitors' web browser allowing for private information to be transmitted without the problems of eavesdropping, data tampering, or message forgery. – *SSL Shopper*

Back in the day the Internet and email were wonderful, care-free tools. Spammers, spoofers and other crooks killed that. But if you will practice some defensive moves, you can still get a lot done on the 'net. We sure do.

Carl Brown is President of GettingGreatRates.com, which specializes in water, sewer and other utility rate analysis and tools. The firm also serves as the RATES Program rate analyst for the Kansas, New Mexico, North Dakota, Virginia and Wyoming rural water associations. Contact: (573) 619-3411; info@gettinggreatrates.com