Don’t Be Scammed By Email Spoofs

You may get these email spoofs sometimes. They come from friends, but contain only a link to some site you’ve never heard of. Sometimes they have a subject line like, ‘You have to see this,” or “Check this out!”

What’s happening is that spammers have gotten their hands on the e-mail addresses of people you know and are “spoofing” e-mails. Spoofing is when the header is altered so it appears to come from somewhere other than the actual source.

Since you probably wouldn’t consider clicking on an e-mail link from a stranger, they’re hoping that seeing a familiar name will trick you into clicking. They can do it because the main protocol used for sending e-mail (SMTP) doesn’t always have an authentication mechanism. That means tech savvy hackers can get in there and use that server to send messages. They can fake an e-mail message to say it’s from any sender or any person. That’s why you sometimes see spam that appears to come from you.

These scammers could get the names of your contacts with Malware installed on your PC, so always keep your security software up-to-date. They could also get the names from the contact list of someone who shares contacts with you, through a malware infection or from someone who likes to include the e-mail addresses of everyone they know in the address when they forward something. And it’s also possible that they’ve managed to hack an e-mail service. So it doesn’t hurt to change your password regularly.

Unfortunately, there’s not a lot you can do. Make sure you report these messages as spam. It does teach your e-mail what to filter out. If it gets to be too much, you can consider changing your e-mail address.