MARKETING MATTERS
WINTER 2014

How Do Spammers Get Your Email Address?

We all use spam filters. Every company we sign up to, whether it's for free newsletters, financial services or online shopping, promises never to share your data with anyone. So how are people who want you to buy dubious meds, unlikely stocks or even more unlikely get-rich-quick schemes getting your email address?

Unfortunately, the nature of the internet is such that it's almost impossible to protect an email address from spam entirely for any length of time.

The easiest way for a spammer to get your email address is by getting hold of a leaked account database. It happens more often than you'd expect – over the last few years, Adobe, LinkedIn, eHarmony, Gawker, Last.fm, Yahoo!, Snapchat and eve the mighty Sony have lost hundreds of thousands of users' details each. These leaked databases are assessed first and foremost as a security threat, because they'll often show account names and passwords. But they usually also show email addresses, meaning spammers can download them and have a readymade address book to send out their phishy emails to. Spammers will know that the majority of these addresses will actually be active, so these databases represent a great catch for them.

That accounts for the majority of cases where you've never given away your details but somehow spammers have found your address anyway. There are websites, like haveibeenpwned?, that will tell you if your account information has been leaked, but these sites won't include every leak. And your email address is in some ways more vulnerable than any password, because you can use different passwords everywhere – but you pretty much have to use the same email address everywhere.

The other big way for spammers to get your address is to scrape the web for email addresses, picking up on the ones that are mentioned on websites in much the same way as search engines scrape for content online. This method is getting less popular now, since many sites use an internal contacting system or assign users a temporary email address to beat spam, and spammers have huge leaked contacts lists to use instead.

If you do get spammy emails, there are things you can do to keep the volume low. Spammers use bugs to see is you're interacting with their emails, so they know if your account is active. If you click on 'unsubscribe,' legit businesses unsubscribe you. Spammers identify your email account as active and step up the pressure. It's the same if you load images: images are often used as a way for spammers to check whether you're opening your emails or not. Even if a visible image doesn't load, there's often a tiny tracking bug that does register your click.

So what can you do to stay spam-free? Don't give out your email address online, don't interact with spam if you get it, and consider having a 'signing up for things' email address and a personal email that you never use to sign up to any business, so the only way hackers can get it is if your email provider is hacked or leaks.

*Submitted to the Greater Ocean Township Chamber of Commerce by GOTCC member **John Kalli, CEO of Trinity Worldwide Technologies.** Trinity takes care of your IT and stands out for their reliability and responsiveness, focus on your needs, and personable staff who serve as your long-term business partner. **www.Trinityww.com 732.780.8615***