COMPUTER NEWS from the

JANUARY 2015 Volume 3 NO.1

As found on the web and other sources

HAPPY NEW YEAR

How Spammers Get Your Email Address

Category: Spam From “askbobrankin.com”.

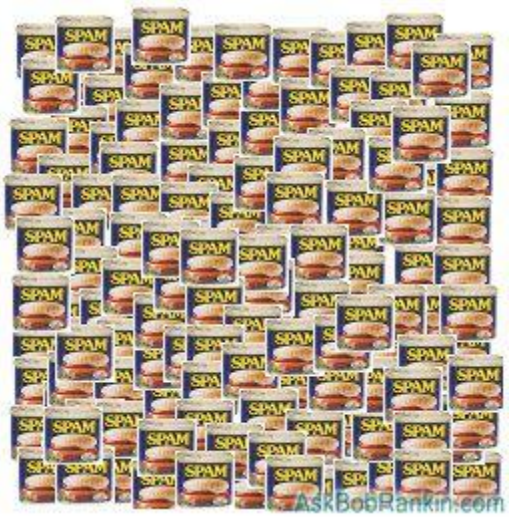
Spammers seem to have supernatural powers that enable them to guess email addresses accurately and quickly. But in reality, spammers harvest email addresses by pretty mundane means. You may even be contributing to the problem without realizing it. Here's the scoop on how spammers get email addresses, and steps you can take to protect your inbox...

Is Your Email Address Vulnerable to Spammers?

It can be maddening when your email inbox gets a fresh load of spam dumped into it. Equally frustrating is when spammers spoof your address as the sender, and your friends all start asking why YOU are sending them unwanted sales pitches for dubious products. Understanding how spammers get a hold of your email address can help to prevent both of these problems.

Using web-crawling "spider" programs (not unlike the ones Google uses to index Web pages) spammers hunt down email addresses by looking for the telltale "@" symbol. Working swiftly and ceaselessly, spiders can harvest millions of email addresses automatically. To avoid being bitten by a spider, don't put your email address on the Web. That means not posting it to online forums or personal web pages. If it's included in online directories (school, work, clubs, etc.) ask to have it removed.

Scan the web with a Google search to see where your email address is available, and work towards becoming invisible. If you must make your email address visible in public, you can obscure your address by avoiding the "@" symbol, i.e., use "joe at blow dot com" instead, or create an image with the address instead.



"Dictionary attacks" are another standard way to collect email addresses. Spammers generate emails to made-up 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.

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 jsmith123@aol.com or susie90210@hollywood.com I can guarantee that 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.

TorrentLocker Ransomware Spreading Fast: Report

By Brandon Dimmel on December, 18 2014 in “Infopackets.com”.

A new report from security firm ESET finds that the TorrentLocker ransomware scam has now encrypted an estimated 285 million files. Unfortunately, ESET security experts don't see the rate of infections dropping off any time soon.

A TorrentLocker infection, like other ransomware schemes (such as **CryptoWall** or **CryptoLocker**), usually takes place when a victim downloads a malicious file. Although the name TorrentLocker might suggest infections come through the way of torrents (a file typically used for file sharing), it does not; in fact, most TorrentLocker infections come through email.

ESET says the people behind TorrentLocker have become remarkably adept at devising spam emails that grab and hold a target's attention; this includes emails about unpaid invoices, traffic violations, and **mailed packages with tracking numbers**. In most cases, the emails are tailored to a target's home country, making them even more believable.

TorrentLocker Rapidly Spreading Around the World

Once the infection is set, TorrentLocker encrypts a victim's files, making it impossible for users to access them. At that point, cybercriminals behind the ransomware demand the victim pay a ransom -- usually a few hundred dollars -- to regain control of their system.

ESET's report shows that there have been just under 40,000 TorrentLocker infections around the world, representing roughly 285 million files. TorrentLocker first emerged in Australia this past August, making its rapid growth alarming to security experts. ESET's study indicates that TorrentLocker has now spread to many other countries, including Canada, the United Kingdom, Italy, Germany, France, Holland, Spain, Turkey, the Czech Republic, and Ireland.

So far there have not been any reports of TorrentLocker infections in the United States, though it's expected infections will emerge there soon. (Source: **pcworld.com**)

Victims Must Pay Bitcoin Ransom to Retrieve Files

The ESET report also notes that, of the roughly 40,000 TorrentLocker victims, 570 have agreed to pay the ransom, representing a 1.4 per cent conversion rate. In most cases this ransom must be paid in Bitcoin, a virtual currency.

In one widely reported case, the computer system of Bussoleno, Italy's town council was infected by TorrentLocker. Without consulting PC security experts or law enforcement officials, the councillors paid the ransom of approximately 400 euros (or roughly $500 USD). Although the payment allowed the Bussoleno councillors access to their files, security experts do not recommend negotiating with cybercriminals. (Source: **techworld.com**)

Overall, it's estimated that the cybercriminals behind TorrentLocker have netted themselves around half a million U.S. dollars using the scam.

I hope no one was caught by this scam!

Shop Online? Watch out for Fake Email Order Scam

By Brandon Dimmel in Infopackets Email Newsletter on December, 9 2014

A new report suggests that hackers are using fake email orders with malicious links to fool victims into installing malware onto their machines. Security experts are therefore warning all Internet shoppers to take extra care when opening their emails this holiday season.

According to Brian Krebs, a former Washington Post writer who covers cyber crime, the problem is becoming more and more prevalent. "If you receive an email this holiday season asking you to 'confirm' an online e-commerce order or package shipment, please resist the urge to click the included link or attachment," Krebs notes on his blog. "Malware purveyors and spammers are blasting these missives by the millions each day in a bid to trick people into giving up control over their computers and identities." (Source: **krebsonsecurity.com**)

Asprox Spam Botnet Harvests Personal Information

Security experts at Malcovery, a firm that monitors email-based malware threats, say that many hackers are currently using this tactic to spread the Asprox spam botnet. Once a system is infected, personal information is harvested from the victim's PC (including passwords, and possibly credit card data); the PC then becomes part of the spamming botnet to propagate itself onto other machines.

Malcovery says people should look out for subject lines that read the following: "Acknowledgment of Order," "Order Confirmation," "Order Status," "Thank you for buying from [insert merchant name here]", and a "Thank you for your order."

Scammers Getting Better at Designing Fake Emails

The tactic is essentially 'phishing,' or the use of legitimate-looking emails designed to convince victims to click on malicious links. Craig Young, a security researcher at Tripwire, says past phishing campaigns were easy to spot because the scams looked so incredibly fake and often contained obvious spelling errors. But that's changing, Young insists.

"Scammers have become incredibly good at making fraudulent emails look legitimate to the untrained eye," Young said. "Attackers will commonly flood the web with spam mail claiming you have a package waiting to be picked up, an order awaiting confirmation, and a plethora of other emails designed to get users to click links." (Source: **pcworld.com**)

Busy People Easy Targets during Holiday Season

The holiday shopping season is particularly lucrative for phishing scammers who know that people are expecting lots of emails confirming their purchases through online retailers, such as Amazon. That makes it far easier to trick people into clicking on a fishy email link. Ken Westin, who also works in security at Tripwire, says hackers "are able to take advantage of people's impulsive nature more easily during this time of year."

Should I remove old .NET Framework?

By Dennis Faas in “infopackets.com”.

Infopackets Reader Dan F. writes: Dear Dennis,

When I run Windows Update, it tells me there are .NET Framework 3.5 updates available. Should I install these Windows Updates, even though my computer has .NET framework 4.5? Also, should I remove old .NET framework (versions 1, 2, etc) from the Windows Control Panel? Or will it cause problems? "

My response:

I recommend installing Windows Updates as soon as they are available (for the reasons I outlined in the comments section of yesterday's article), as the latest Windows Updates usually address bug fixes or security-related issues. Without installing the latest Windows Updates, your system may be exploitable and can result in **malware infection**, **or worse**.

Should I Remove Old .NET Framework?

You can remove the old versions of .NET framework on your system if you wish, but doing so comes with caveats.

Most likely you have a program already installed on your system that requires a specific version of .NET framework. If you remove the wrong .NET framework (whether it's version 1, 2, etc), some programs may no longer function. That said, newer versions of .NET framework are most likely not backwards compatible with older versions of .NET framework.

Case and point: an old program I use, "RSS Reader," requires .NET framework version 1. The author of the program did not know that the latest version of .NET framework version existed (currently version 4.5) because the program is more than a decade old, and because .NET framework version 1 was the only version available at the time. As such, this program specifically requests .NET framework version 1 during install on my system. Therefore, this particular program won't work with .NET framework 4.5, though technically it may be compatible.

If you insist on only using the newest .NET framework (for whatever reason that may be), you will have to figure out which programs use the old .NET framework and uninstall / replace them with newer programs that provide similar functionality and / or that do not require .NET framework to function.

How to know which program requires which .NET Framework?

Unfortunately there's no easy way to know which programs require which .NET (that I know of), though there may be some freeware program available that can provide this sort of detective work. If you uninstall a .NET framework and then launch a program that happens to require the .NET you just uninstalled, you will most likely receive a Windows error message stating that some sort of .DLL file is missing and that the program can't launch.

If you type in the .DLL error message into Google (example: "somefile.dll not found", or such), the search results will usually point you in the right direction. After clicking on a few pages, I'm sure you'll come across one that will tell you that you are missing .NET framework required to run the program. In that case, you can simply uninstall the broken program with a replacement.

DO YOU BELIEVE THIS?

Humans generate only 38.5 percent of all Web traffic; the rest of the Web pages served are requested by bots both good and bad. Search engines are “good” bots and generate 31 percent of Web traffic. Malicious bots such as content scrapers, hacking tools, spam bots, and mysterious “other bad non-human traffic” account for the remaining 29.5 percent

---

I thought this program might prove useful to some.

I take no responsibility!

SPAMfighter 7.6.87 Keep spam out of your inbox with SPAMfighter, a unique tool specially built for Outlook, Outlook Express, Thunderbird, Windows Mail, and Windows Live Mail. This free utility is ...

http://www.infopackets.com/news/8934/spamfighter-7687-and-ashampoo-clipfinder-hd-235

A paraprosdokian is a phrase or sentence that leads us down the garden path to an unexpected ending.

Evening news is where they begin with 'Good Evening,'

and then proceed to tell you why it isn't.

That’s all folks!