I've Been Hacked! Or Not.

By Steve Jaffe – January 2019

There isn't a day that goes by in our shop that we don't receive some type of support ticket where a user believes they have been hacked.

Now, what does hacked actually mean? Were you really hacked? How can you tell?

eDot, LLC

3075 Tollview Drive
Rolling Meadows, IL
60008

847 847 4500

www.eDotSolutions.com

Hacked… what does it actually mean?

If you were hacked, it means that someone physically (via remote access) has gotten through your computer or your network security and is able to operate within your computer. Once inside your system, they can do a whole lot of bad things.

What can they do? One of the most devastating hacks is when, unbeknownst to you, data is stolen. This could be e-mail addresses and contacts. This could be copies of e-mails that you sent to clients or financial institutions. It could be information containing bank account numbers, social security numbers, payroll, user names and passwords. Equally as bad is when the hacker encrypts your data and requires that you pay a ransom to get everything back.

Most times, users don't actually know they were hacked as the "bad guy" is working behind the scenes. In some cases we have seen, they put specific rules in your mail system that allow them to receive copies of some or all of your incoming and outgoing mail, which is used for financial gain.

Many articles and people use the word Hack to expand beyond this definition. That's fine. But, the cure and prevention for a true hack is different than other definitions.

Everything above means you were Hacked.

However, in about 100 support calls we receive… maybe 1 is a true hack. Most are not, but they scare the user enough to believe they were.

Let's start at the beginning with different types of electronic communication.

***

Spam – The Good, The Bad, The Ugly

Just Annoying Spam: "The Good"

The easy one that we are all used to seeing: Plain Spam. Spam is just what it is… junk mail. Spam in its truest form is typically worthless mail trying to get you to buy something.

It could be from places you frequent, such as stores or restaurants. They may contain coupons and/or ads since you gave them your e-mail address.

It could be from real businesses with legitimate offers that acquired your e-mail address by purchasing it.

In both cases above, these will typically bypass your Spam Filter. This doesn't mean that you can't Blacklist them or apply them to your Junk mail within your mail system. But, these are not bad e-mails.

Problem Spam: "The Bad"

Now we enter the world of people wanting your money (when you don't get anything in return). You *still* weren't hacked. Millions upon millions of "Bad e-Mails" are sent every day, typically from countries that have no issue with this going on. These are the ones that make wonderful offers of getting rich without any risk, promises of additional growth on your person, medications that solve problems that no reputable physician will confirm, or selling goods/services that are too good to be true.

A good Spam System will block 95% of the Bad e-Mails from ever reaching you.

Destructive Spam: "The Ugly"

The worst of the worst! The e-mail itself makes every effort to lead you to clicking on a link on the page. The words used are creative and made to look like the company may be familiar to you. Perhaps it's from Amazon saying your order was held up… or Microsoft saying you are required to verify your account or you will be shut off. The best ones are those that use proper language and familiar references.

Clicking that link will start a chain of events that are difficult to undo in most circumstances.

How can you identify these?

a) If you think there's the remote possibility that this is NOT a legitimate e-mail, call your IT Person and don't delete the e-mail.

b) Move your cursor over the link (<u>DO NOT CLICK</u>). Look at the domain address that pops up. If it's bad, you will see a really strange domain address.

c) Call the company on the e-mail. Ask if they sent anything to you. (PS – don't use the phone number on the e-mail… look it up on the web.)

What can happen if you click the bad link? (Choose any or all)

1. Malware is installed.
2. Ransomware locks up your Device until you pay the ransom.
3. Data gets stolen if you fill out their form or reply with the information they asked.

Now, if all of this happens above, were you "hacked"? Not really, although it would seem so to the user. No one is actually inside your system

But, if you do accidentally provide them the information they seek, here's what may lie next for you:

4. Rules are set up to forward any and all e-mails you received/sent.
5. Your entire Contact Database is stolen (and then used for future use by the "bad person").
6. If your Computer has access to your Server, they may be able to do further damage.

Will my Protection Licenses stop this from happening? In many cases, yes. As long as the proper licenses are installed and up to date. But, you should never rely on those licenses in place of vigilance.

***

Spoofing

The basic definition of Spoofing is when someone tries to impersonate your e-mail address, your name or your IP Address. Think of this like a telemarketer who spoofs a local area code so when you look at your incoming Caller ID, you see an area code that is familiar to you. So, you are more likely to answer it (vs. an 888 area code). That's what these people are trying to do with Spoofing in an e-mail. They want the recipient (YOU) to open the e-mail and feel comfortable enough to hopefully do whatever they want you to do:

a) Fill out a form to steal your personal information (so they can come back later and hack into your computer)
b) Transfer money to some off shore account
c) Click a link that will install bad stuff on your computer

I've Been Hacked!

So, when you get a very real phone call from your family, friend, client, or vendor that says they got an e-mail from YOU asking them to send you money or fill out some form and it has YOUR NAME and YOUR EMAIL address in that e-mail, you believe you were hacked.

I understand why, but you probably were not.

This is a typical Spoof e-mail. And, sadly, there is virtually nothing you can do about it, except tell your family, friend, client, vendor that it isn't real and to tell their IT department or just delete it. Perhaps they can blacklist the IP Address from future e-mails (but good hackers change IP addresses frequently).

Now, these types of e-mails go in phases… there was the one a couple years back where a family member or friend would ask you to send them, via Western Union, some money because you lost your wallet and are in a foreign country.

More recently, the bad person finds an e-mail address within your company that asks you to wire money to a vendor (they are real good at finding who the CFO and Controller are within companies). Just look at your own company web site and see if the CFO/Controller is in the About Us section!

How can you tell if you received a real or spoofed e-mail?

If this is a bad attempt at spoofing, look at the return e-mail address. It won't be the correct one. Look at the spelling of the name… is it correct? Call the person and verify it came from them.

The more serious investigative method is to review the header information on the e-mail (or just forward the e-mail to your IT Department). Header Information gets a little complicated and you need to know what you are looking for. But, within that header, an IT person can frequently determine if this is real or spoofed.

Header Information

In Outlook, open the e-mail

Then, go to File Properties.

If you have ANY suspicions that this e-mail isn't good, don't click on anything and definitely don't reply. Get it to your IT Department.

***

Can I Prevent Any of This?

The definitive answer is…

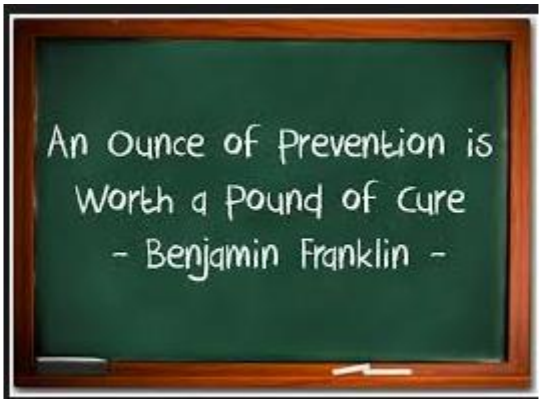
Your e-mail address is out in the Internet World. Maybe your e-mail address is also on your company web site, or in an article you wrote, on a social media site, or in one of the dozens of big name companies whose data was stolen (along with your information). Your e-mail address is also in the address book of tens, hundreds or thousands of people (many of whom had their address book compromised at some point).

You can't really prevent your name or e-mail from being Spoofed by others. It's just not possible. But, you can implement several steps to reduce your susceptibility to being compromised.

1. MAKE SURE, you have all necessary protection licenses on your computer. Make sure the virus definitions are ALWAYS up to date.
2. MAKE SURE your company has a content filtering program installed.
3. MAKE SURE your company has a Geo Fencing filter on your Firewall.
4. Check your Rule Set in your mail program to ensure that there are no rules that you did NOT implement (especially ones that auto send and auto delete).
5. Use a complex password that is a minimum of 10 characters in length. Change it frequently.
6. Search out an on-line class on how to identify bad e-mails (for yourself or for your company).
7. Review your company security protocols to ensure they are current.
8. Confirm that your firewall has no open ports.
9. Implement a multi-factor system for remote users.

And, if you still believe you were hacked…

#1 – Change your password IMMEDIATELY.
#2 – Run all your available Malware/Ransomware programs for viruses.
#3 – Check your e-mail rules
#4 – Do NOT rush to e-mail the entire world that you were hacked and to not open e-mails from you.
#5 – Tell your IT Department and await their instructions.



***

This Article is the 2nd in a Series focusing on Network Security.
Please go to our web site for all articles (www.eDotSolutions.com)

About the Author

Steve Jaffe is the Co-Founder and active Partner of eDot, LLC a large Managed Services Provider located in the Chicago Area. Mr. Jaffe has a BS in Business Administration and a Master's Degree in Corporate Finance. He has been President and/or CFO of over a half dozen mid-sized companies in the previous 20 years. Mr. Jaffe, along with his business partner, Melvin Thoede, Jr. own a Managed Services Company, a Telecommunications Company, a Surveillance/Access Control Business, and a Web Development/Programming Agency.

Outside the office, Mr. Jaffe is a husband to a middle school teacher, father of four teenage children, a pilot, a chef, a writer and a voracious reader.

About eDot, LLC

eDot, LLC is a large Managed Services Provider (MSP) serving businesses and school districts with 1 to 500 employees in the Midwest and throughout the United States. For information on our services or for more information on our Client Security Programs/Audits, go to www.eDotSolutions.com for complete contact information.