BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle
May 2019

End Of Support Notifications Being Sent To Windows 7 Users

If you're still clinging to your old Windows 7 machine, you should know that the day is relentlessly drawing closer wher Microsoft is going to stop supporting the OS altogether. In fact, in the near future, you're going to start seeing reminde pushed out by the company that the end is drawing near. They're calling this a "courtesy reminder" and recommendin an upgrade to Windows 10.

If you're dead-set on continuing to use Windows 7 past the date when official support ends, Microsoft is offering an additional three years of paid support for the platform. However, the price of that support will double with each passing year.

The company has taken pains to continue supporting what is still a surprisingly popular operating system. However, given all of the above, the writing on the wall is pretty clear to see at this point.

If you haven't yet begun to make plans to move away from your legacy systems that require Windows 7 to function, it's well past time to do so. When the support stops, you're going to find yourself at increasing risk. The hackers around the world are going to find flaws in Windows 7's armor and Microsoft isn't going to be around to fix them.

Even worse, an increasing percentage of modern software simply won't run on those older systems, which puts you in an increasing bind on that front. You would have to buy separate systems to run the newer software you need, while maintaining a few of the older boxes to house and run the software that depends on the older OS. That complicates things, to say the least.

The longer you delay, the worse those risks are going to become. Painful as it might be to consider moving away from the platform, the alternative is worlds worse. Time and technology have simply moved on.

Get More Free Tips, Tools and Services At Our Web Site

www.biz-net.com

(775) 850-7700

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

Malware In Documents Is The Latest Hacker Trend

There is a new Threat Spotlight released by Barracuda Networks.

One of the biggest trends in 2019 (where threats against businesses of all sizes are concerned) now takes the form of poisoned documents attached to emails.

The company analyzed more than 300,000 email samples collected over the past twelve months.

They discovered that the frequency of document-based malware attacks increased markedly during the first quarter of 2019, with nearly sixty percent of poisoned files taking the form of documents.

As Jonathan Tanner of Barracuda Networks put it:

"For the past couple of years, script files were a very popular attack method. The percentage of these sort of files declined drastically, however, and was a significant source of the increase of documents as an infection method...

Documents are a natural evolution from script files, since the languages used are also the ones used for documents - namely VBScript and JavaScript. The same attacks could be converted to the document-based ones with only slight modifications. The script authors had already become very adept at obfuscation techniques, so these could contribute greatly to document-based malware where scripting is already more common and thus deeper inspection of the script itself is required."

The good news is that most antivirus software is quite good at detecting malicious files. Of course, the weakest link in the equation isn't detection software, it's users. In light of the evolving threat, education is more important than ever. Although to date, the majority of employees have been stubbornly resistant to educational measures designed to reduce the rate at which employees will click on and open documents received from un-trusted or even unknown sources.

As a business owner, that will likely be one of your great challenges in the year ahead. The more wary you can make your employees about opening files from people they don't know, the safer your network is bound to be.

- Light bulbs in the New York City subway system screw in "backwards" (i.e. with left-handed threads) so that people can't steal them to use at home.
- Janet Airlines is a highly classified airline that shuttles military personnel in and out of Area 51. The name stands for 'Just Another Non-Existent Terminal'.
- Movie theatre popcorn is sold at a 1275% markup
- The word 'bus' is actually short for 'omnibus' meaning "To contain many things" and didn't originate until the early 19th century.
- Volkswagen sells more sausages than cars, sold under the "Volkswagen original parts" number 199398500a, the currywusrt has been available for 45 years now.
- The Olympic flag's colors are always red, black, blue, green, and yellow rings on a field of white. This is because at least one of those colors appears on the flag of every nation on the planet.
- Japan is giving its elderly population discounts on ramen if they give up their drivers' licenses.

New Phishing Attack Targets Amex And Netflix Users

If you do business with either American Express (AMEX) or Netflix, be on the alert. Windows Defender Security Intel has recently reported the detection of two major new phishing-style campaigns aimed at the customers of both businesses.

Recipients have been receiving emails that appear identical to official Netflix and American Express communications.

In both cases, the ultimate goal is to convince customers to hand over their credit or debit card information. Microsoft has sent a couple of different tweets out about the issue. One of them assures customers that "Machine learning and detonation-based protections in Office 365 ATP protect customers against both campaigns."

And another warned that "The Netflix campaign lures recipients into giving away credit card and SSN info using a 'Your account is on hold' email and a well-crafted payment form attached to the email."

The unfortunate truth is that emails like the ones currently in play are extremely easy to craft and very compelling. The hackers simply play on the fears of the customer, making it sound as though if they don't take immediate action they'll lose access to a valued service they've come to rely on.

There's essentially no cost to the hacker for pushing out hundreds, or even thousands of emails like the ones currently being used. For each victim that falls prey to the tactic, the costs can be enormous.

As ever, the first best line of defense is education and awareness. In addition to that, if there's ever any question at all about the status of your account, the best thing you can do is to address the issue via another channel.

In other words, don't simply reply to the email you received. Open a new tab, look up the company's customer support number and call to verify. Doing so will tell you in short order whether the email you received was legitimate, or someone trying to separate you from your hard-earned money.

Protecting Yourself From Phishing Attacks

In almost all cases, opening and reading an email or message is fine. For a phishing attack to work, the bad guys need to trick you into doing something. Fortunately, there are clues that a message is an attack. Here are the most common ones:

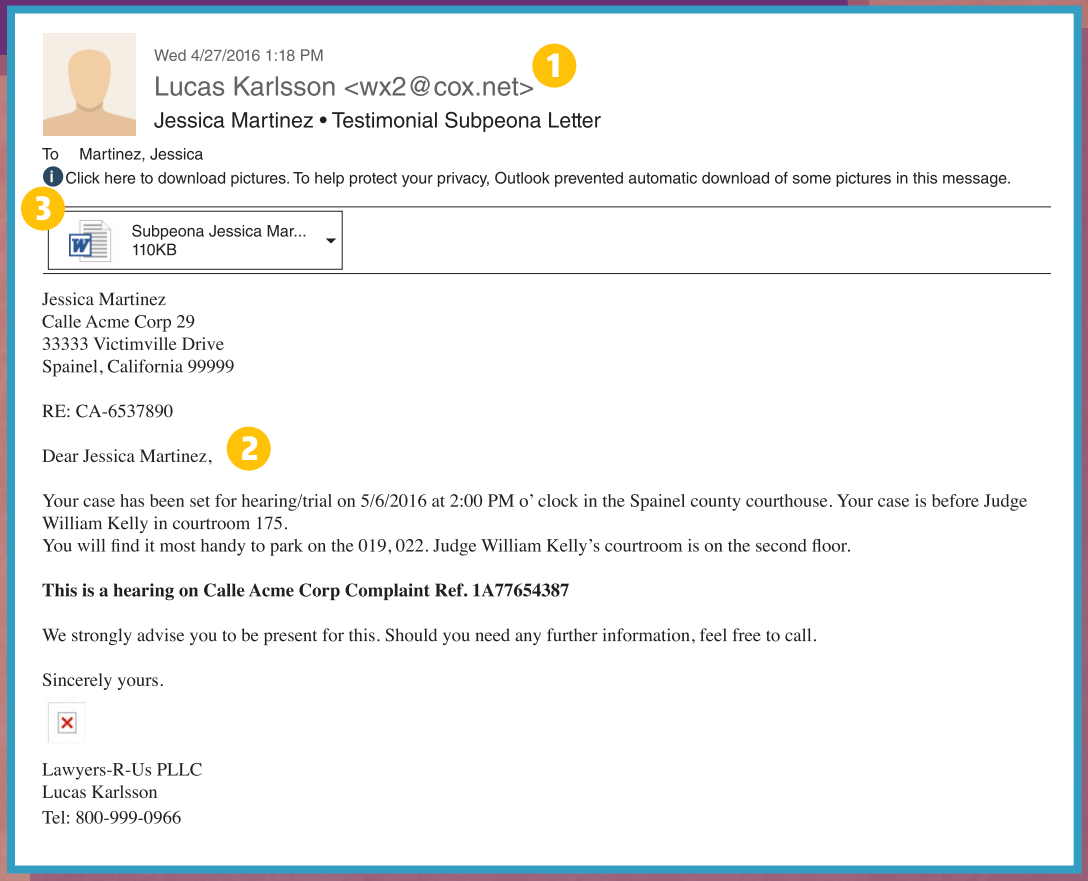
- A tremendous sense of urgency that demands "immediate action" before something bad happens, like threatening to close an account or send you to jail. The attacker wants to rush you into making a mistake.
- A strong sense of curiosity or something that is too good to be true. (No, you did not win the lottery.)
- Requesting highly sensitive information, such as your credit card number, password, or any other information that a legitimate sender should already know.
- The message says it comes from an official organization, but has poor grammar or spelling or uses a personal email address like @gmail.com.
- The message comes from an official email (such as your boss) but has a Reply-To address going to someone's personal email account.
- You receive a message from someone you know, but the tone or wording just does not sound like him or her. If you are suspicious, call the sender to verify they sent it. It is easy for a cyber attacker to create a message that appears to be from a friend or coworker.

Ultimately, common sense is your best defense. If an email or message seems odd, suspicious, or too good to be true, it may be a phishing attack.

A Real Life Spear Phishing Attack

Are you familiar with spear phishing? You should be, because the spear phisher is familiar with *you!* Unlike phishing emails that are usually sent at random from an aggregated list, spear phishing targets specific people. A spear phisher knows your email address, the company you work for and just enough information about you and your position that he or she can use that information to appear to be a friend, a colleague, a boss or even law enforcement!.

What does a spear phishing attack look like? Here's a real life example below. *(Actual names and information have been changed.)*



Wed 4/27/2016 1:18 PM

Lucas Karlsson <wx2@cox.net> 1

Jessica Martinez • Testimonial Subpeona Letter

To Martinez, Jessica

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

3 Subpeona Jessica Mar... 110KB

Jessica Martinez
Calle Acme Corp 29
33333 Victimville Drive
Spainel, California 99999

RE: CA-6537890

Dear Jessica Martinez, 2

Your case has been set for hearing/trial on 5/6/2016 at 2:00 PM o' clock in the Spainel county courthouse. Your case is before Judge William Kelly in courtroom 175.
You will find it most handy to park on the 019, 022. Judge William Kelly's courtroom is on the second floor.

This is a hearing on Calle Acme Corp Complaint Ref. 1A77654387

We strongly advise you to be present for this. Should you need any further information, feel free to call.

Sincerely yours.

Lawyers-R-Us PLLC
Lucas Karlsson
Tel: 800-999-0966

At first glance, the email to the right seems legitimate. It addresses the recipient by name. The signature includes a phone number. The body of the email includes Jessica's actual place of employment. **So how would she know this is a scam?**

1 Let's start at the top. Who is Lucas? And why does his email address look so strange? His name isn't in the email address, it doesn't look professional and if it were actually from Lawyers-R-Us PLLC, wouldn't the domain name reflect that?

2 This is the first Jessica is hearing of any sort of testimonial or legal issue. Why would she be subpoenaed out of the blue and via email at that? Wouldn't her supervisors or company lawyers inform her of such things well before she was advised to appear in court?

3 Finally, doesn't it seem strange that there's an attachment when everything she needs to know is written in the body of the email? What is it for?

This very well-crafted spear phishing attack hits all the right notes. If Jessica had let her **fear** take control without studying the email closely, she may have downloaded the attachment and launched it on her work computer, infecting it with malware.

What should you do if you receive an email like this?

At home: delete, delete, delete. At work: follow policy, know how to report any security incidents and, if you're not sure, ask someone immediately!