Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

Is That eMail for Real?

The easiest way for hackers and ransomware to mess with your computer is social engineering. Basically, that means ‘Wear the appropriate repair-guy uniform, walk into the building looking confident, and go directly to the system that you will be "fixing." No one challenges that, right?

OK, well then, would you click on this email? I don't remember ordering a pricy server from Amazon, but it looks like I'm getting one. I guess I'd better look in there and see who ordered it for me; could be that my account was hacked.

From Amazon.com <amazon@amazons.com>
Subject **Your Amazon.com order has shipped (#425-21882237-4858555802)**

amazon

Shipping Confirmation

Hello,

Your order "Dell PowerEdge T430 5U Tower Server - 1 x Intel Xeon E5-2620 v4 Octa-core (8 Core) 2.10 GHz - 8 GB Installed DDR4 SDRAM" has shipped.
Below you can find the invoice and the shipping details.

Details

Order #425-21882237-4858555802

Expected delivery date:
February 22, 2017
Total including shipping:
$1628.99

Order details

Depending on the ship speed you chose, it may take 24 hours for tracking information to be available in your account.
We hope to see you again soon.
Amazon.com Unless otherwise noted, items sold by Amazon.com LLC are subject to sales tax in select states in accordance with the applicable laws of that state. If your order contains one or more items from a seller other than Amazon.com LLC, it may be subject to state and local sales tax, depending upon the seller's business policies and the location of their operations. Learn more about tax and seller information on our website.
This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

So what's wrong with it? Here goes, most obvious and visible items first:

- I ordered no such thing.

- The sender's email address has the wrong domain, ‘amazons.com' which is also not the web address for Wonder Woman's family island. The return address for Amazon orders is generally auto-confirm@amazon.com.
- The format of the email is simpler than the usual Amazon shipping confirmation, missing gray backgrounds, logos, and a picture of each item ordered. It looks a lot like an Amazon confirmation from ten years ago.
- The order number is not a text link in the email, and the last section has too many numbers.
- "it may take 24 hours for tracking information to be available in your account." No, tracking shows up in Amazon before the email is sent; it's Fedex and UPS that will just say ‘label printed' until the next morning.
- Finally, not visible above, if you float your mouse over the ‘Order Details' button, which is missing the orange logo that Amazon would normally use, you will see the link, which goes to usintecmedical_ com_br, not Amazon. That ‘com.br' points to a site in Brazil, probably hacked.

What to do? Will this big Dell system show up at my door? No. I **TYPED** ‘amazon.com' into my browser, didn't follow the link, and checked. No surprises there. However, that medical address in Brazil would likely have looked like an Amazon page, asked for a login, which it would keep and use, and then forwarded you to the real Amazon. Or the site would attempt to install malware. Be suspicious. These fake confirmations can look like they come from nearly any large company.

Windows 10 Free Upgrades End This Month

Although Microsoft stopped the free and nearly-forcible upgrades to Windows 10 a while back, free upgrades are still available up to the end of December 2017, for users of Windows 7 and 8 or 8.1, if they would like to use any of the Accessibility Features that are in Windows 10. These include the screen reader (Narrator), Magnifier, cursor and pointer size changes, high contrast themes, and even the personal assistant Cortana.

If you would like to use any of these features, the upgrade page is here:
https://www.microsoft.com/en-us/accessibility/windows10upgrade
Or call me for help. Remember to always back up before upgrading. Use a ‘system' or ‘image' backup to a USB hard drive.

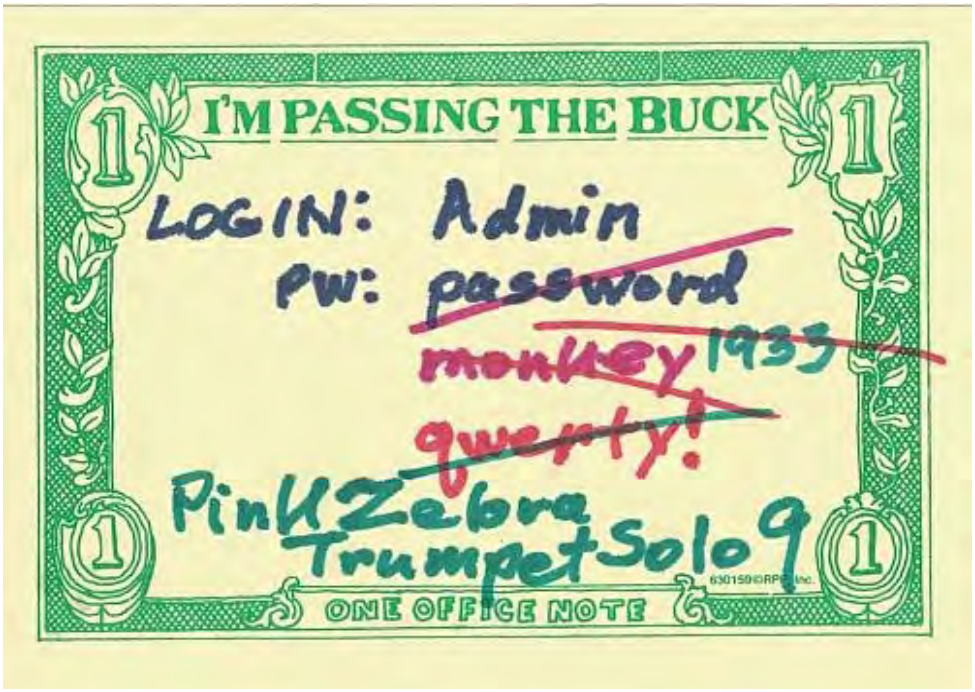
Windows 7 Updates Broken, Again, Fixed, Again.

Microsoft let a date run out in their Windows 7 updates as of December 3rd, and it broke the connection to Windows Update. As of now, that date was patched at Microsoft, and updated for 2025, so updates should be running again. If Windows 7 isn't updating, call me, and I can give it a swift kick in the software updater.

Reminder: Windows 7 Security Updates are still scheduled to end in January 2020, just 25 months from now. If you still have Windows 7 computers, plan ahead.

Choosing Passwords, One More Time

Online passwords to financial sites are important, and you have to choose passwords carefully.



I continue to hear that passwords are difficult to remember. No, not unless you chose something that's gibberish. Again, the best passwords are long, and easy to remember. For example, which password is more secure, but which one is easier to remember?

- pa$$w0rd8
- stupidpurplepassword

Mathematically, the longer stupid password is vastly superior to pa$$w0rd8, by a factor of 383 billion to 1, possibly much higher.

Why? Well, the short answer is that length is far more important than complexity, so don't stress about upper, lower, number, and symbols, and just use a long set of words, at least 12 characters. There's math behind that, but it qualifies as a review of probability class.

To adapt the purple password to something that even a mis-informed bank will actually approve, try something like: PurplePassword#7

Again, it's the length that's most important, not how many different letters and symbols are in it. If an attacker KNEW that you only used lower case, or only upper case, it would make his job much easier, but they don't know that. Most sites are now insisting on different character types, but the characters don't have to be nonsense or random.

So my long-term recommendation stands: Use passwords you can easily remember, three unrelated words are the easy way. Anything memorable above 12 characters is excellent, as long as you can type it in easily, and as long as it is used in only one place.

And for the "Don't" list--hackers expect these:

- Don't end passwords with the year of any event; they're too easy to guess..
- Don't use family names or initials for passwords.
- Don't use a password at more than one site.
- Don't use single-word passwords.
- Finally, 'password' is not a password. Ever.

Contact

Address all editorial and unsubscribe requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158