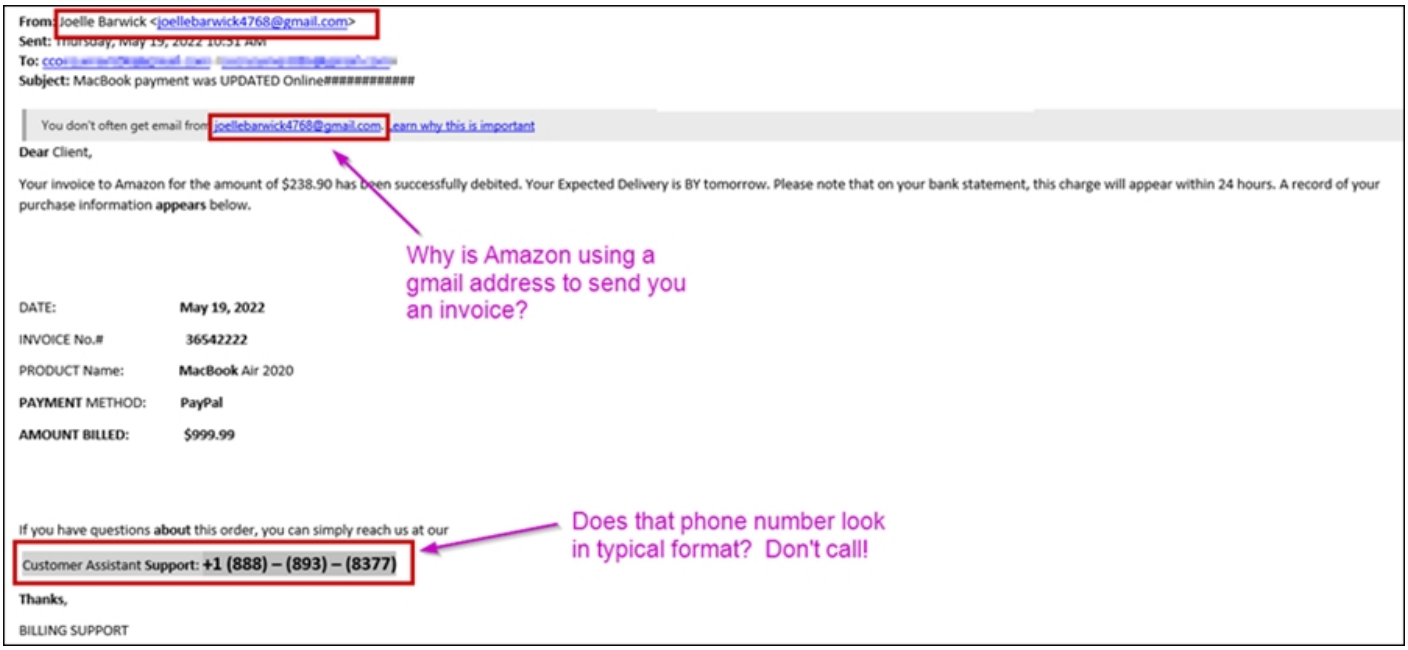
I got a suspicious email, what do I do?

We all get those once in a while, sometimes its easy to tell that its Spam or Ads, or that its even a phishing email, however some look legit and hard to be sure.

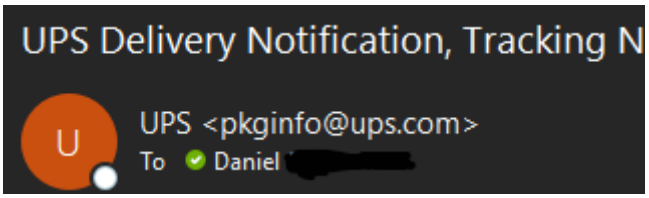
We recommend you to send us a copy that we can review, if you ever do question it, or just unsure.

Always question each email:



Here is few things to look for:

1. The "From" Email Address (this will help you with 99% of them)



everything after the @ symbol matters, does it look correct and same as their website? Most companies will have a website, and if you can type in the address into web browser @ as a website, and it loads, that's usually a good indicator that it is more legitimate email address. For instance this email came from pkginfo@ups.com so if I take whats after the @ symbol and try to go to ups.com and it loads a whole website and looks legitimate, then likely is a more legitimate website. However this DOES NOT Apply to @gmail.com @yahoo.com @outlook.com as they are email host providers and anyone can make an email address and make it look more legitimate.

If Microsoft is emailing you, it should be @microsoft.com and same for most companies, if its something else, its a red flag already.

If its a big company and coming from a @gmail.com, then 99.99999% chance its a fake or scam.

2. Does it have unusual grammar?

   Yes, large companies can get hacked too, or have their domain "spoofed". So its important to look at email carefully and see if it has unusual grammatical errors, that is not normal for size of company.

3. Is it asking you to do something unusual?

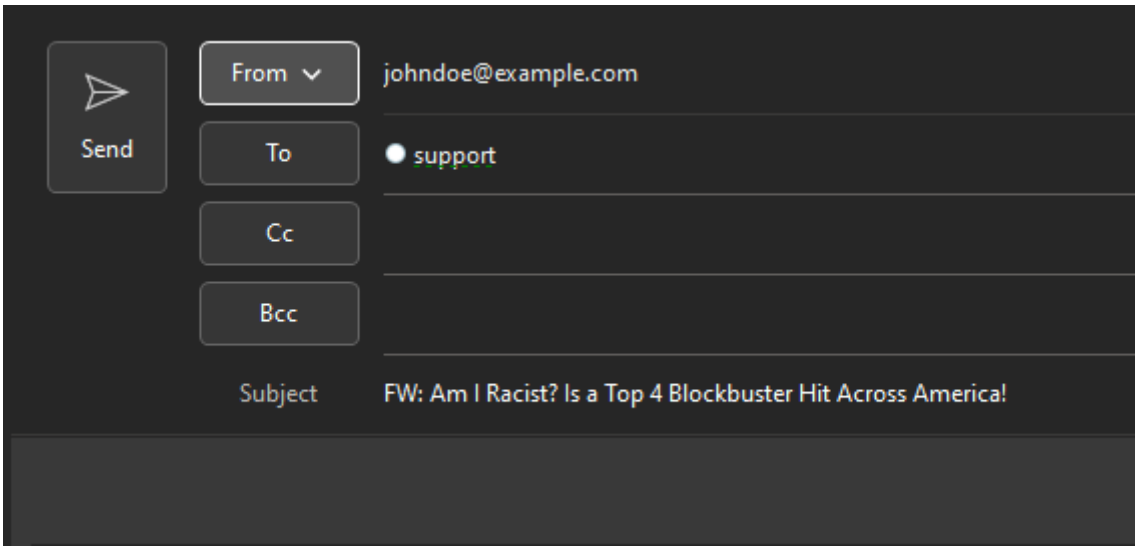
   Is the attachment a pdf or word document and sending you to login to your Microsoft account? **then likely a phishing attack.**

   Is it asking you to update billing information with company you don't normally have that arrangement or you do already have it set and they are asking you to update it? Most of these scammers want to get your money, they are usually going to find creative ways for you to get them your banking information.

   > Use an alternative method to verify this request, call with number you have for that company (NOT the one they include in that same email) and ask if they really sent that email. You never know if their email got hacked and if that party did send that email or not, better to be sure.

Best way to send copy to us:

Simply click to forward it, and send to support@precision-computer.com



If you may, attach the Internet Headers in the email, to help determine where it was routed from - Follow this link for How do I find the Email Internet Headers?

Revision #5
Created 16 September 2024 21:26:23 by Daniel O
Updated 21 March 2025 13:52:40 by Daniel O