Indentifying a Phishing Email

What is phishing?

This technique is called **phishing**, and it’s a way hackers con you into providing your personal information or account data. Once your info is obtained, hackers create new user credentials or install malware (such as backdoors) into your system to steal sensitive data.

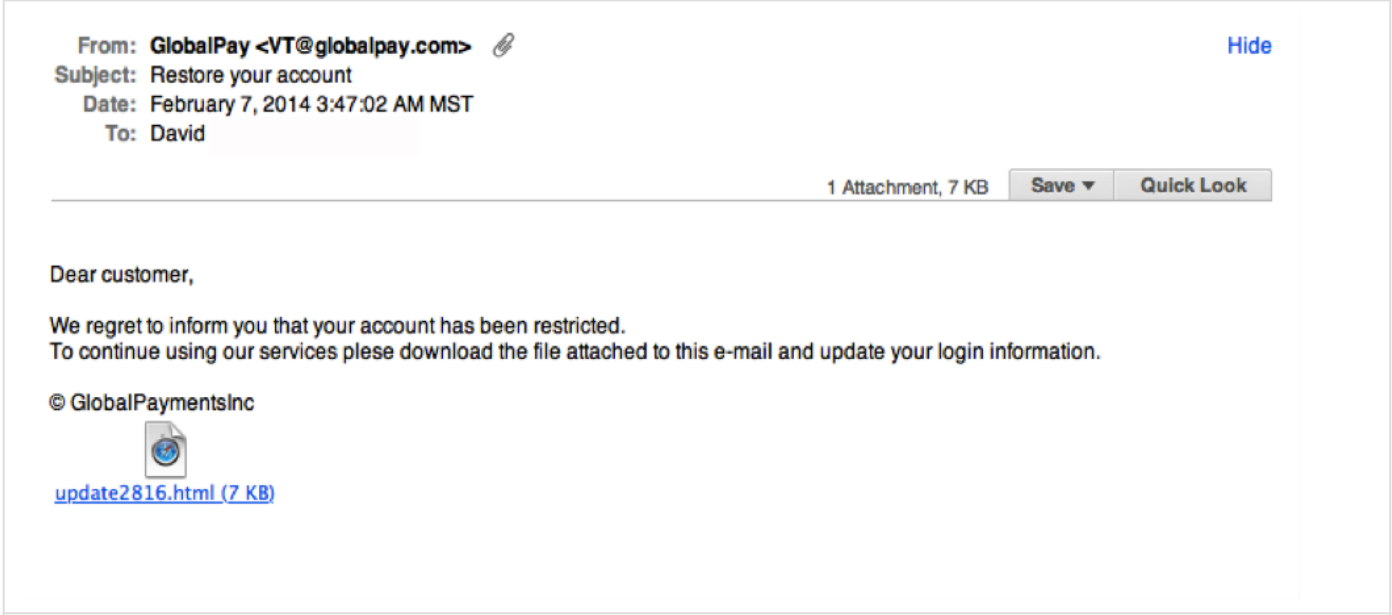
Phishing emails today rarely begin with, "Salutations from the son of the deposed Prince of Nigeria..." and it's becoming increasingly difficult to distinguish a fake email from a verified one. But, most have subtle hints of their scammy nature. Here are seven email phishing examples to help you recognize a malicious email and maintain email security.

Email phishing examples

Are you sure that email from UPS is actually from UPS? (Or Costco, BestBuy, or the myriad of unsolicited emails you receive every day?) Companies and individuals are often targeted by cybercriminals via emails designed to look like they came from a legitimate bank, government agency, or organization. In these emails, the sender asks recipients to click on a link that takes them to a page where they will confirm personal data, account information, etc.

1. Legit companies don’t request your sensitive information via email

Chances are if you receive an unsolicited email from an institution that provides a link or attachment and asks you to provide sensitive information, it’s a scam. Most companies will not send you an email asking for passwords, credit card information, credit scores, or tax numbers, nor will they send you a link from which you need to login.



Notice the generic salutation at the beginning, and the unsolicited web link attachment?

2. Legit companies usually call you by your name

Phishing emails typically use generic salutations such as “Dear valued member,” “Dear account holder,” or “Dear customer.” If a company you deal with required information about your account, the email would call you by name and probably direct you to contact them via phone.

BUT, some hackers simply avoid the salutation altogether. This is especially common with advertisements. The phishing email below is an excellent example. Everything in it is nearly perfect. So, how would you spot it as potentially malicious?

Confirmation of your request from Hotels.com MISC/Scams ×

Hotels.com <Hotelscom@roktpowered.com> Nov 14, 2018, 11:38 AM (1 day ago)
to dave

Hotels Hotel Deals Packages & Flights Groups Customer Service Gift Cards Secret Prices

Hotels.com™

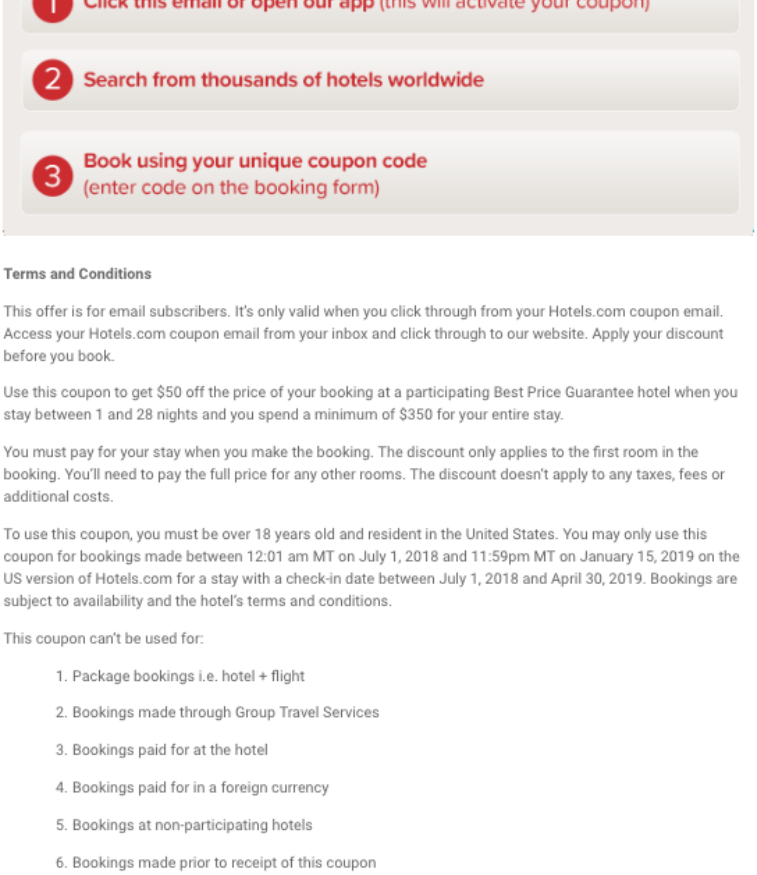
New York Hotels Las Vegas Hotels Chicago Hotels Los Angeles Hotels

EMLRKUSH21850:SK7CM6 Book now

You must click through this email or book through our app to redeem this coupon.

*Use by 11:59 PM MT on 01/15/19 for travel by 04/30/19. Can't be used on some hotels. See details below.

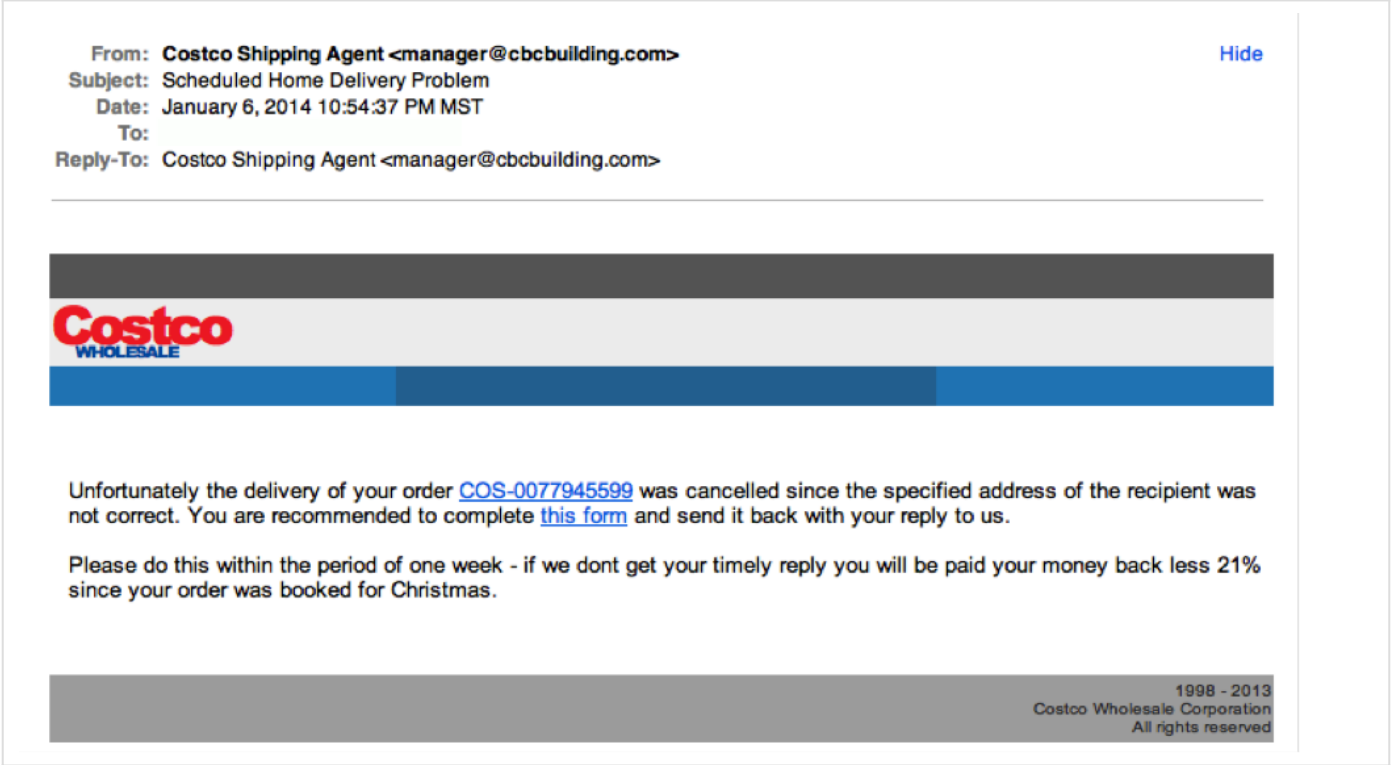
Bookings using this coupon are not eligible for Hotels.com™ Rewards.



This is a very convincing email. For me, the clue was in the email domain. More on that below.

3. Legit companies have domain emails

Don’t just check the name of the person sending you the email. Check their email address by hovering your mouse over the ‘from’ address. Make sure no alterations (like additional numbers or letters) have been made. Check out the difference between these two email addresses as an example of altered emails: michelle@paypal.com michelle@paypal23.com Just remember, this isn’t a foolproof method. Sometimes companies make use of unique or varied domains to send emails, and some smaller companies use third party email providers.



From: **Costco Shipping Agent <manager@cbcbuilding.com>** Hide
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Costco WHOLESALE

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

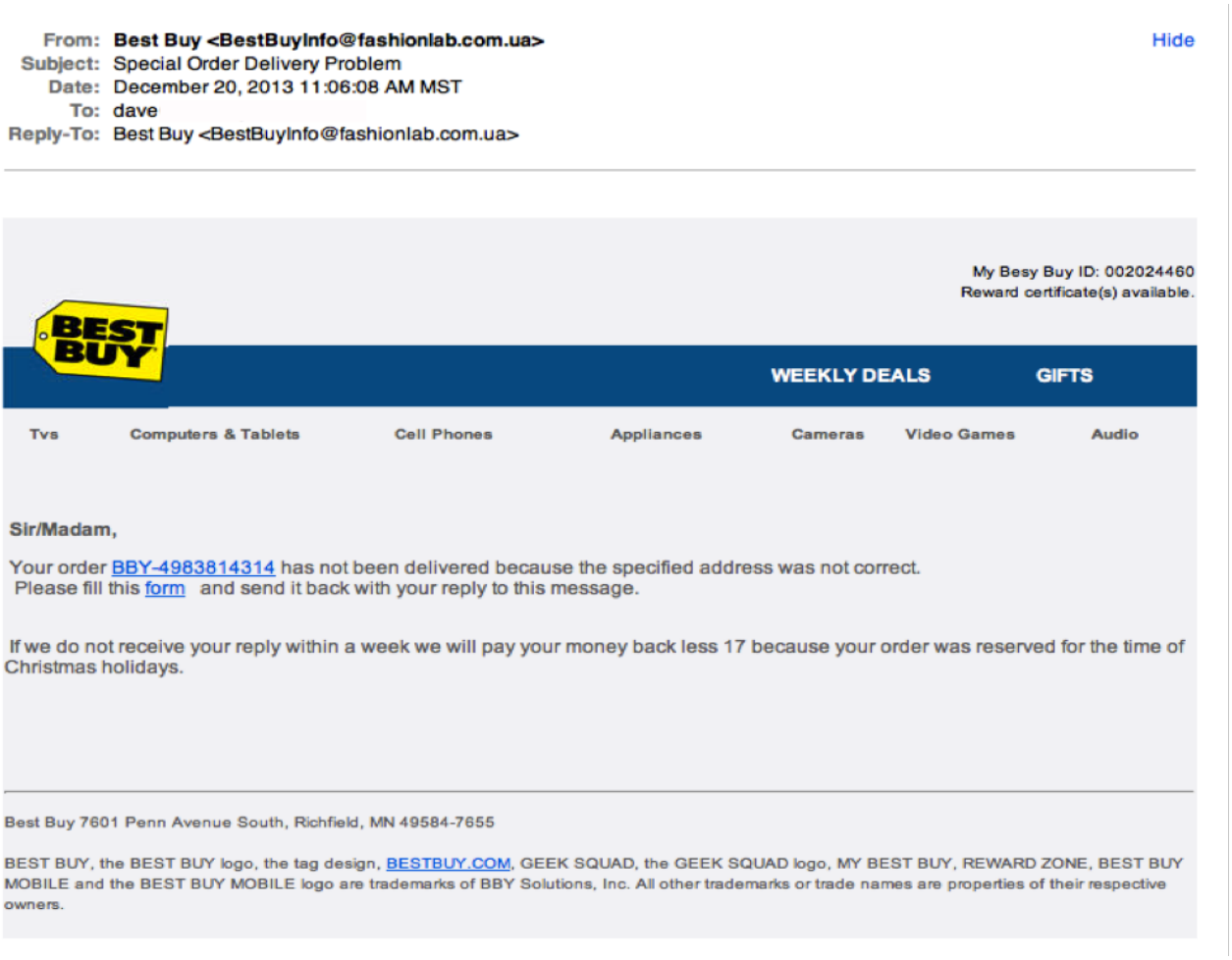
"Costco's" logo is just a bit off. This is what the Costco logo is supposed to look like.

COSTCO® WHOLESALE

See the difference? Subtle, no?

4. Legit companies know how to spell

Possibly the easiest way to recognize a scammy email is bad grammar. An email from a legitimate organization should be well written. Little known fact – there's actually a purpose behind bad syntax. Hackers generally aren't stupid. They prey on the uneducated believing them to be less observant and thus, easier targets.



From: **Best Buy <BestBuyInfo@fashionlab.com.ua>**
Subject: Special Order Delivery Problem
Date: December 20, 2013 11:06:08 AM MST
To: dave
Reply-To: Best Buy <BestBuyInfo@fashionlab.com.ua>

Hide

My Besy Buy ID: 002024460
Reward certificate(s) available.

BEST BUY

WEEKLY DEALS GIFTS

Tvs Computers & Tablets Cell Phones Appliances Cameras Video Games Audio

Sir/Madam,

Your order BBY-4983814314 has not been delivered because the specified address was not correct.
Please fill this form and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

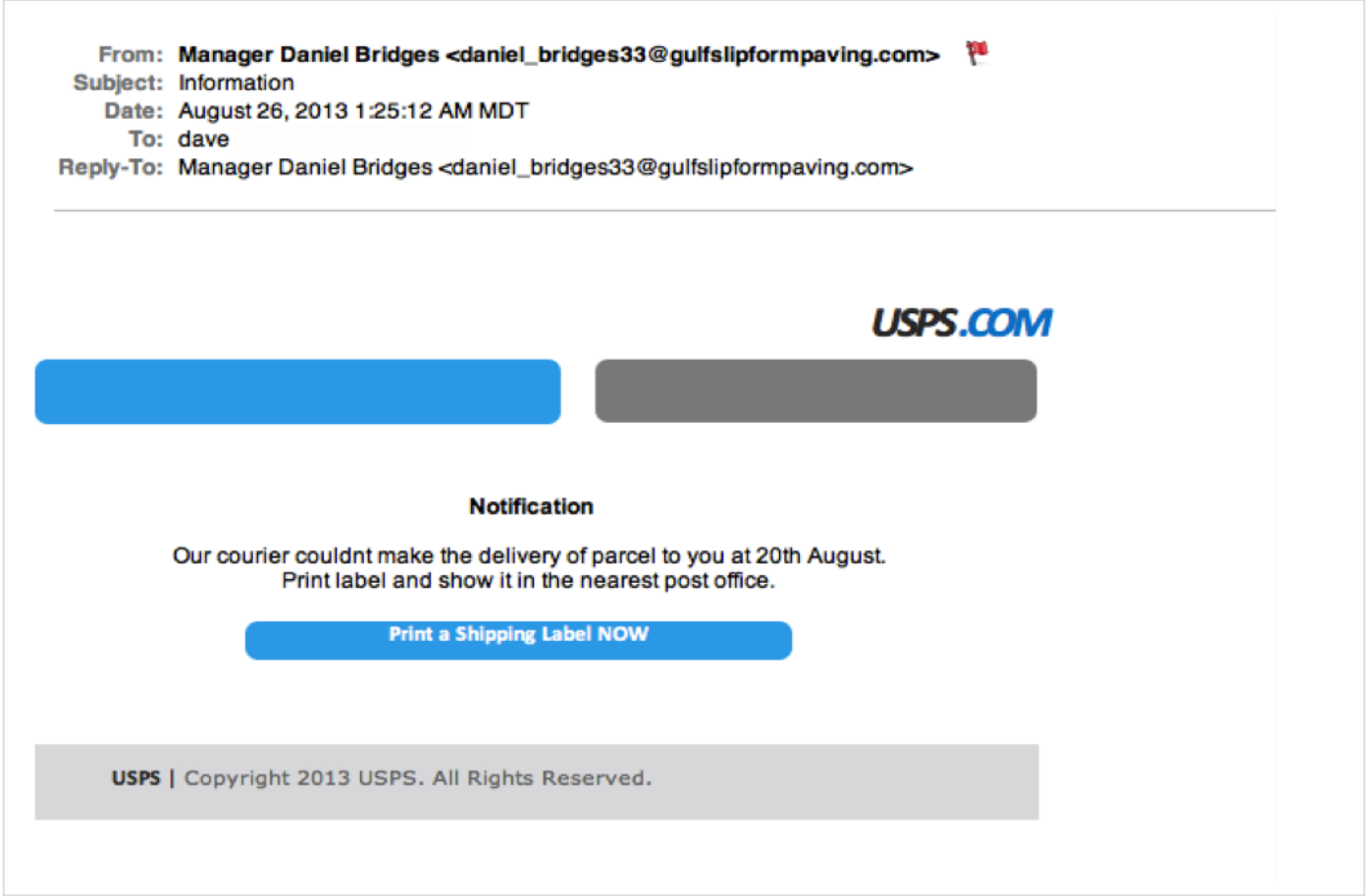
Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, BESTBUY.COM, GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.

In addition to the generic salutation, grammar gaffes are usually a good clue that something is wrong. “Please fill this form…” And notice the ‘17’ reference in the middle of the sentence.

5. Legit companies don’t force you to their website

Sometimes phishing emails are coded entirely as a hyperlink. Therefore, clicking accidentally or deliberately anywhere in the email will open a fake web page, or download spam onto your computer.



*This whole email was a gigantic hyperlink, so if you clicked **anywhere** in the email, you would initiate the malicious attack.*

Revision #1
Created Sat, Mar 28, 2020 4:48 PM
Updated Sat, Mar 28, 2020 4:54 PM