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.

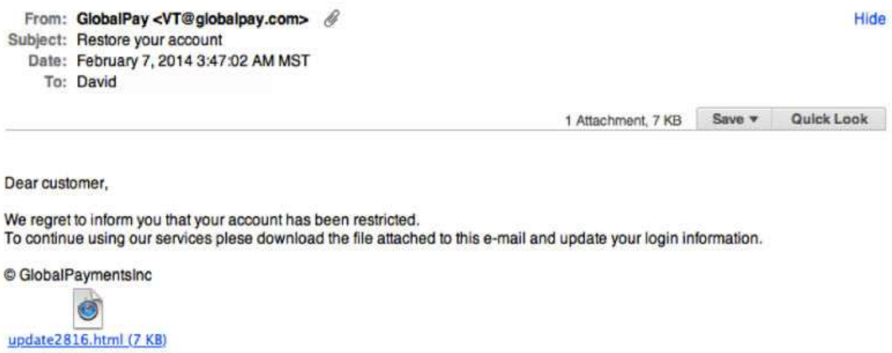
What is phishing?

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…" It's often difficult to distinguish a fake email from a verified one, however 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.

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.



From: GlobalPay <VT@globalpay.com>
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

Dear customer,

We regret to inform you that your account has been restricted.
To continue using our services plese download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc

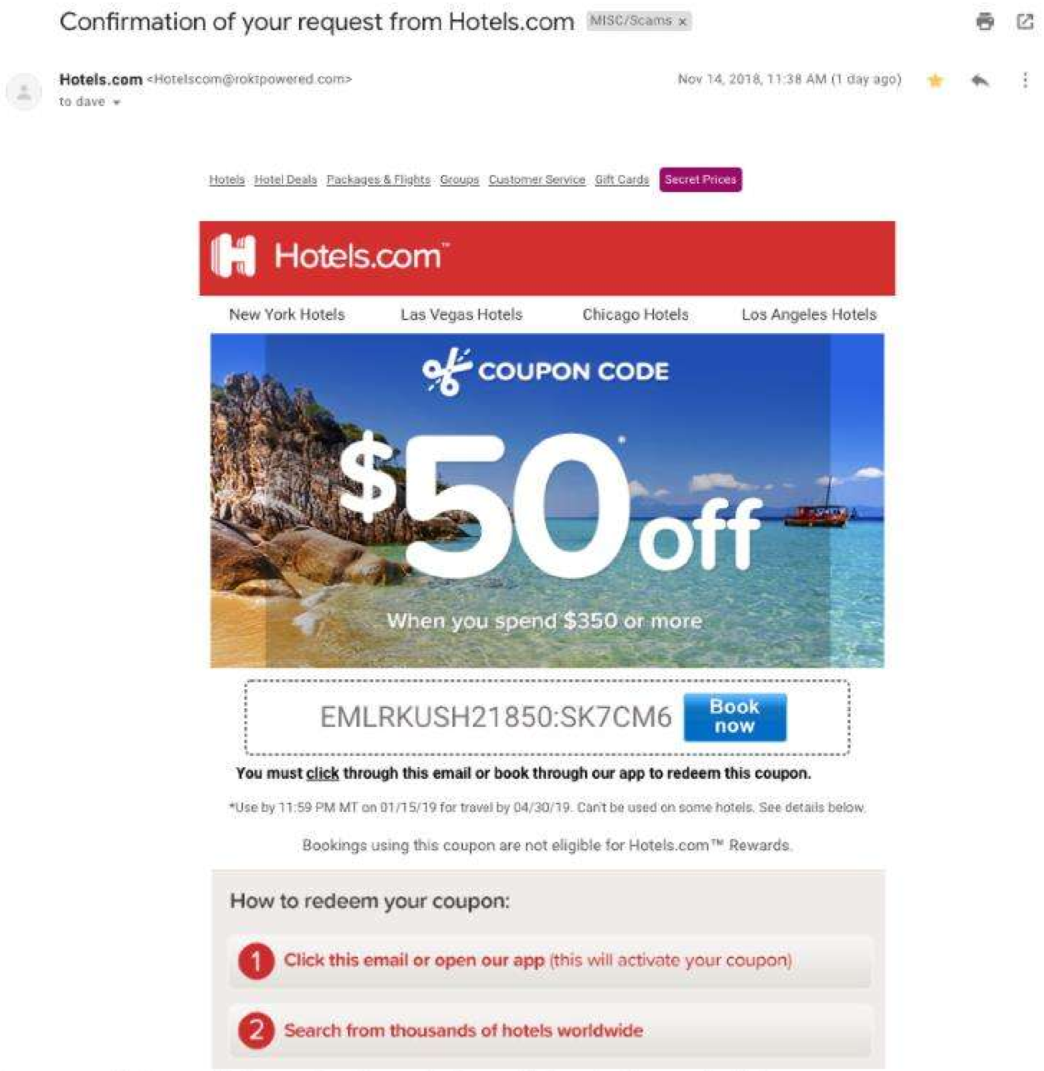
update2816.html (7 KB)

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

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

EMLRKUSH21850:SK7CM6

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.

How to redeem your coupon:

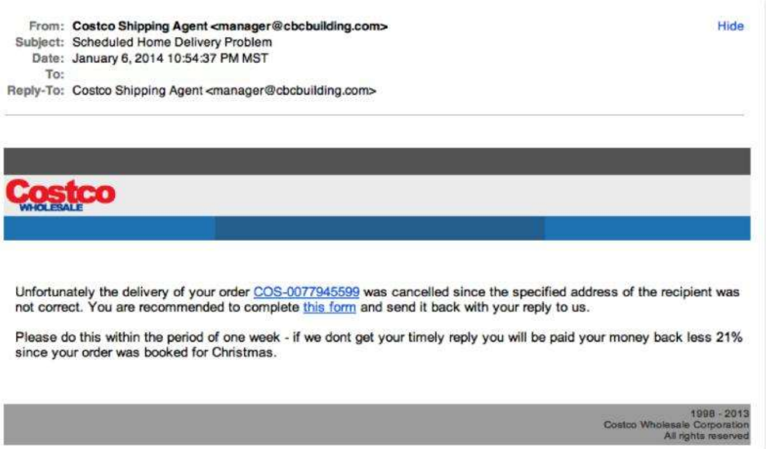
1 Click this email or open our app (this will activate your coupon)

2 Search from thousands of hotels worldwide

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.



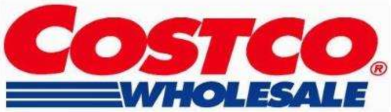
From: Costco Shipping Agent <manager@cbcbuilding.com>
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

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.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

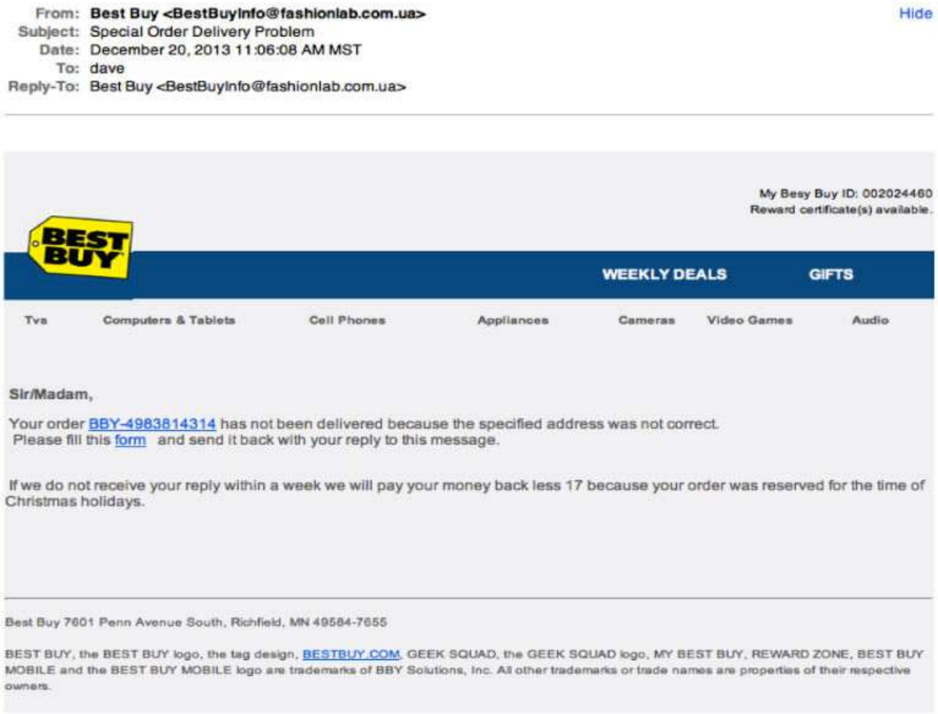
"Costco's" logo is just a bit off. This is what the Costco logo is supposed to look like.



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>

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

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.

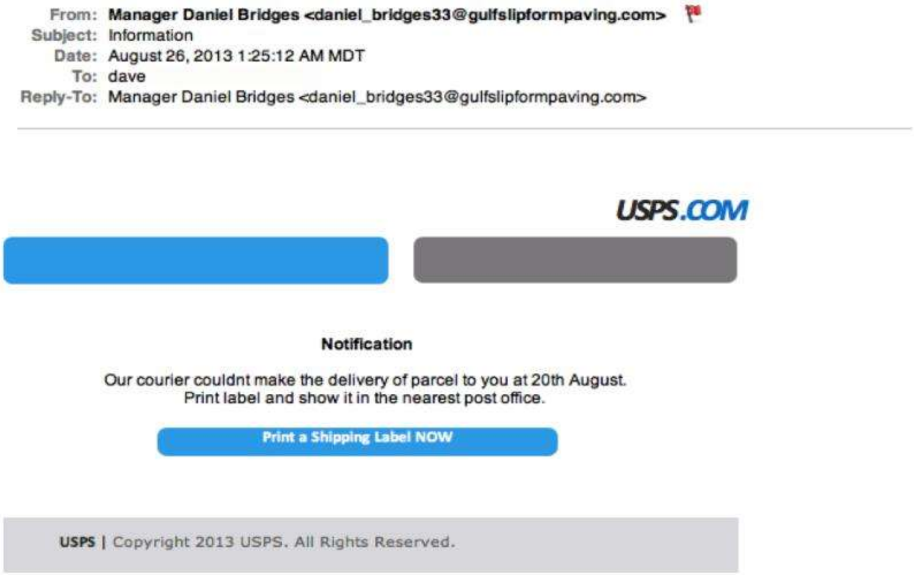
Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

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.



From: Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>
Subject: Information
Date: August 26, 2013 1:25:12 AM MDT
To: dave
Reply-To: Manager Daniel Bridges <daniel_bridges33@gulfslipformpaving.com>

USPS.COM

Notification

Our courier couldnt make the delivery of parcel to you at 20th August.
Print label and show it in the nearest post office.

Print a Shipping Label NOW

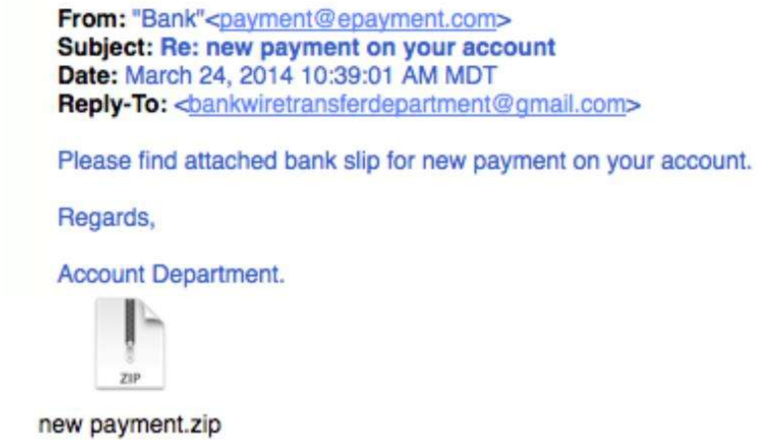
USPS | Copyright 2013 USPS. All Rights Reserved.

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

6. Legit companies don't send unsolicited attachments

Unsolicited emails that contain attachments reek of hackers. Typically, authentic institutions don't randomly send you emails with attachments, but instead direct you to download documents or files on their own website.

Like the tips above, this method isn't foolproof. Sometimes companies that already have your email will send you information, such as a white paper, that may require a download. In that case, be on the lookout for high-risk attachment file types include .exe, .scr, and .zip. (When in doubt, contact the company directly using contact information obtained from their actual website.)



From: "Bank"<payment@epayment.com>
Subject: **Re: new payment on your account**
Date: March 24, 2014 10:39:01 AM MDT
Reply-To: <bankwiretransferdepartment@gmail.com>

Please find attached bank slip for new payment on your account.

Regards,

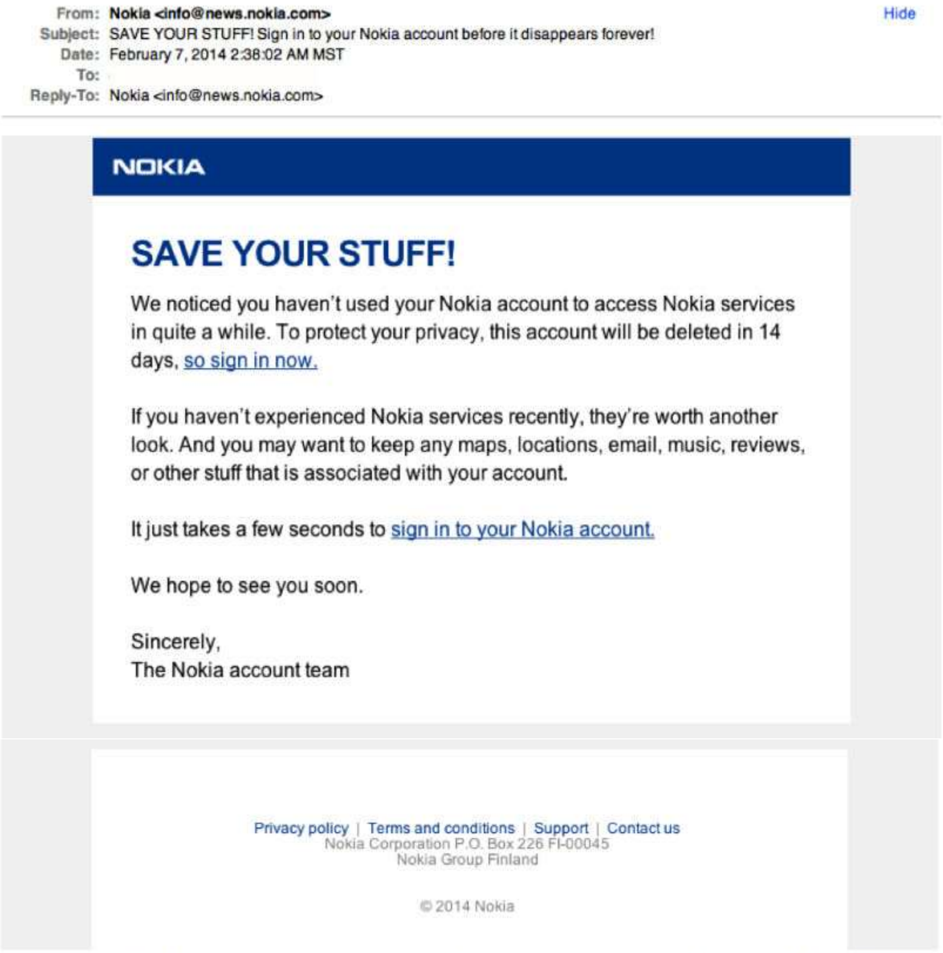
Account Department.

new payment.zip

Just remember, curiosity killed the cat.

7. Legit company links match legitimate URLs

Just because a link says it's going to send you to one place, doesn't mean it's going to. Double check URLs. If the link in the text isn't identical to the URL displayed as the cursor hovers over the link, that's a sure sign you will be taken to a site you don't want to visit. If a hyperlink's URL doesn't seem correct, or doesn't match the context of the email, don't trust it. Ensure additional security by hovering your mouse over embedded links (without clicking!) and ensure the link begins with https://.



From: **Nokia <info@news.nokia.com>**
Subject: SAVE YOUR STUFF! Sign in to your Nokia account before it disappears forever!
Date: February 7, 2014 2:38:02 AM MST
To:
Reply-To: Nokia <info@news.nokia.com>

SAVE YOUR STUFF!

We noticed you haven't used your Nokia account to access Nokia services in quite a while. To protect your privacy, this account will be deleted in 14 days, so sign in now.

If you haven't experienced Nokia services recently, they're worth another look. And you may want to keep any maps, locations, email, music, reviews, or other stuff that is associated with your account.

It just takes a few seconds to sign in to your Nokia account.

We hope to see you soon.

Sincerely,
The Nokia account team

Privacy policy | Terms and conditions | Support | Contact us
Nokia Corporation P.O. Box 226 FI-00045
Nokia Group Finland

© 2014 Nokia

Although very convincing, the real Nokia wouldn't be sending you a "Save your stuff" email from info@news.nokia.com