Southwind

VOLUME 38 ISSUE 1 | www.easasoutheast.org | 1st QUARTER 2019

Register Now for the 2019 "Early Conference"

Registrations are now being accepted for the rescheduled 2018 Fall Conference, also known as the 2019 Early Conference, March 6-9 at the Marriott Resort & Spa at Grande Dunes, Myrtle Beach, South Carolina. You should have received registration information by now, but if you need more information or registration/exhibitor forms, you can find everything you need at the chapter website, http://www.easasoutheast.org/spring-conference/.

Remember, the deadline to reserve your rooms at the contract rate of only $145 per night is February 8! You can book your room by calling 1-800-228-9290 or by following this LINK or the link at the chapter website just above.

Note: Regarding the Spouse/Guest program, it looks like the Waccamaw River Tour will probably go on as planned! Just be sure to bring a jacket.

7 Ways to Recognize a Phishing Email

https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

By David Ellis
Security Metrics

VP, Investigations
CISSP, QSA, PFI

"You can fool some of the people all of the time, and all of the people some of the time, but you cannot fool all of the people all of the time." –Abraham Lincoln

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.

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 ways to help you recognize a phishing 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.

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.

Continued on page 2

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

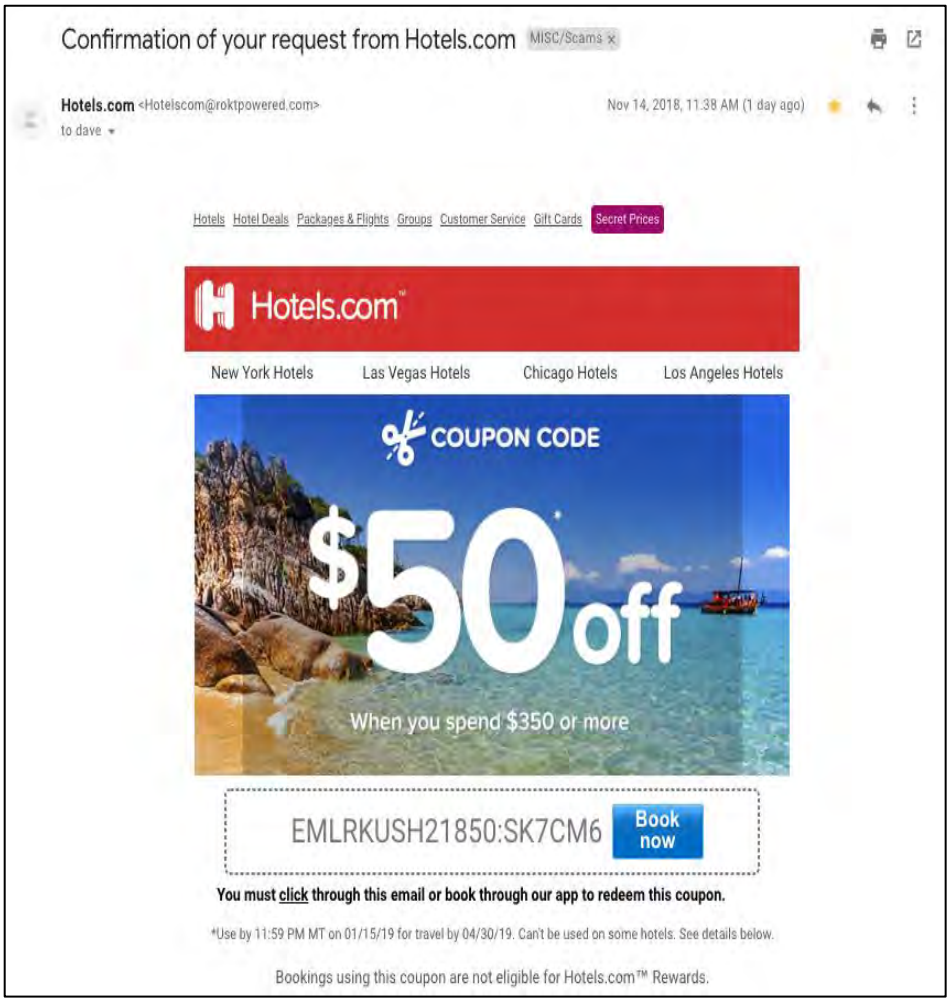
BUT, some hackers simply avoid the salutation altogether. This is especially common with advertisements. The phishing email to the right is an excellent example. Everything in it is nearly perfect. So, how would you spot it as potentially malicious?

3. Legit companies have domain emails

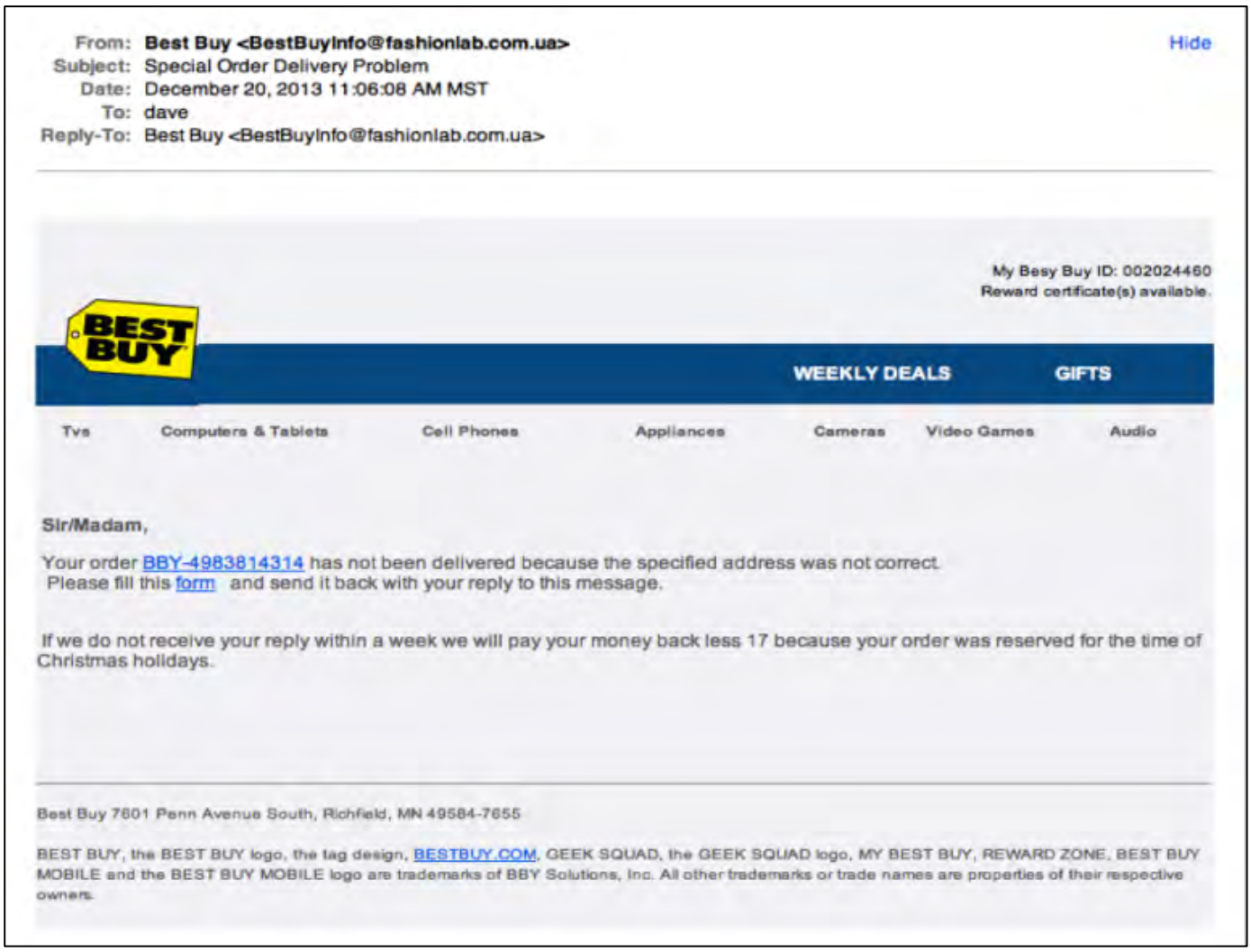
Don't just check the name of the person sending you the email. Check their email address by hovering your mouse over the 'from' address. Make sure no alterations (like additional numbers or letters) have been made. Check out the difference between these two email addresses as an example of altered emails: 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.

4. Legit companies know how to write and 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.



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



From: **Best Buy <BestBuyInfo@fashionlab.com.ua>** Hide
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.

BEST BUY

WEEKLY DEALS GIFTS

Tvs Computers & Tablets Cell Phones Appliances Cameras Video Games Audio

Sir/Madam,

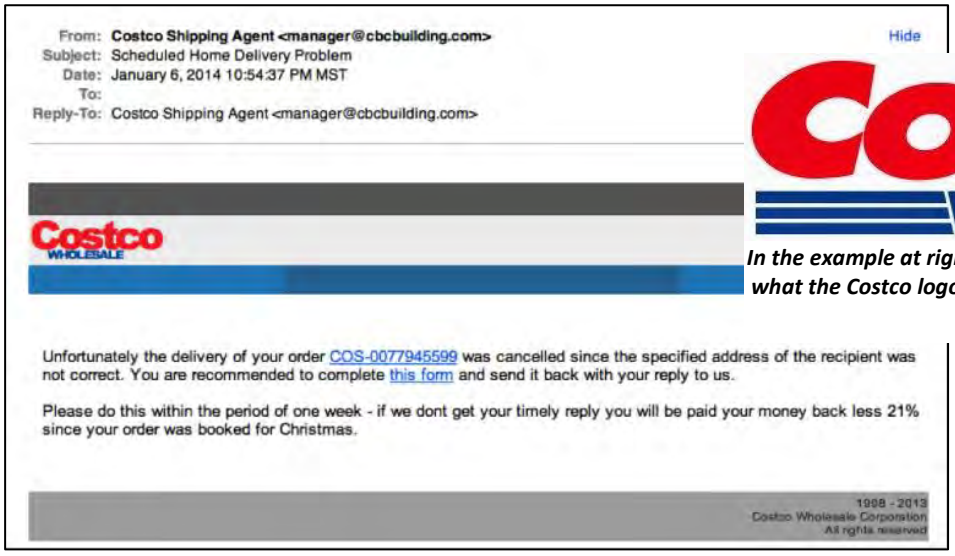
Your order BBY-4983814314 has not been delivered because the specified address was not correct.
Please fill this form and send it back with your reply to this message.

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.

[Note from the Southwind Editor: if the text sounds like it was composed by someone in Russia or Ukraine, there's a good chance it was.]



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.

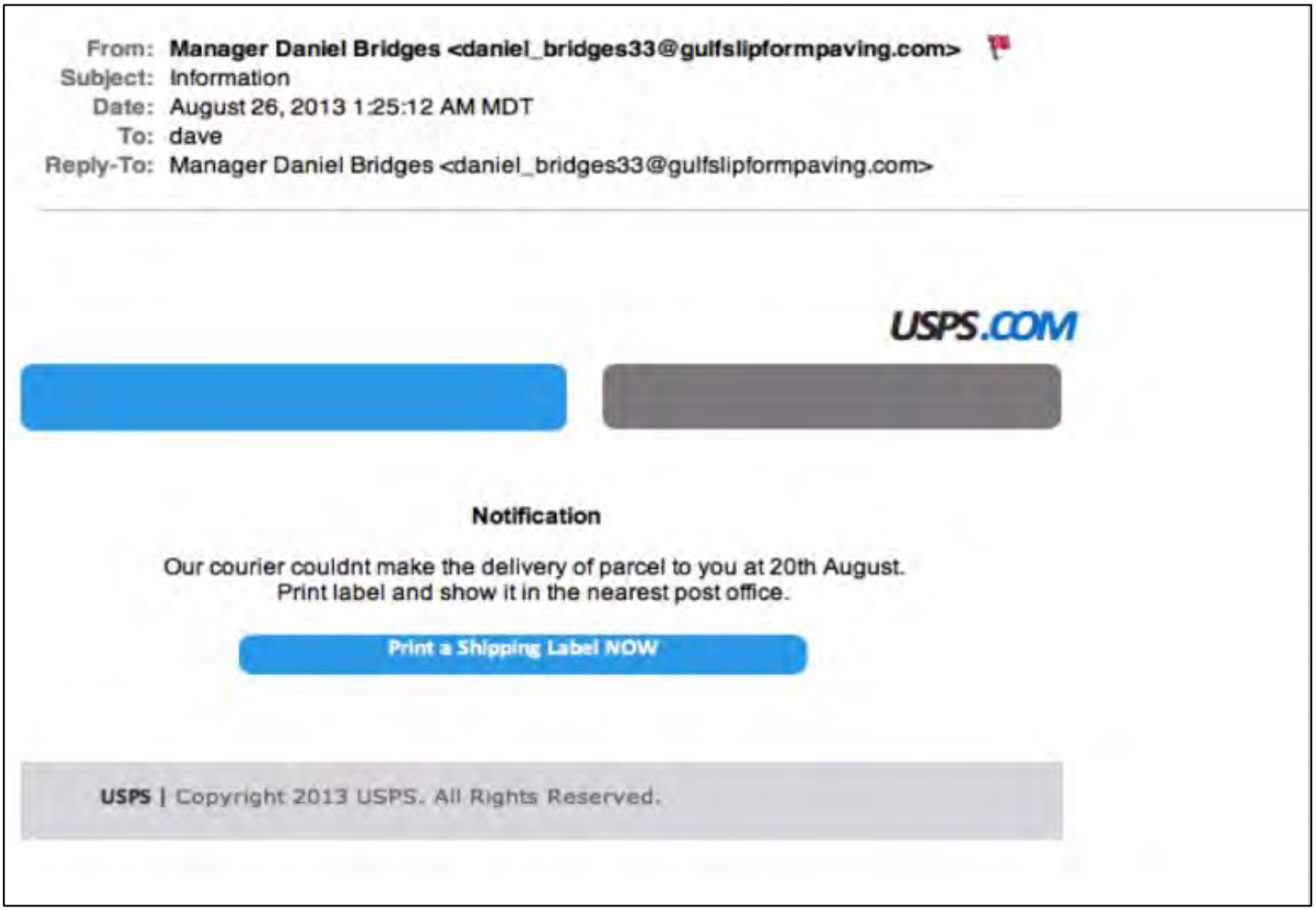
Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

In the example at right, "Costco's" logo is also just a bit off. This is what the Costco logo is supposed to look like. See the difference? Subtle, no?

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.



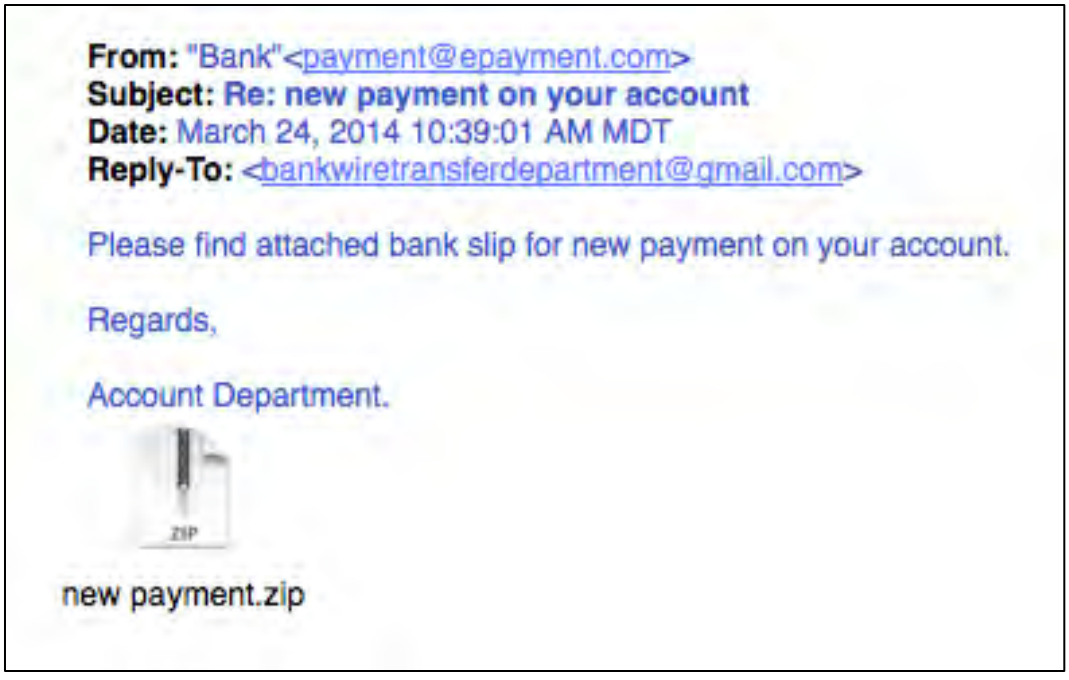
This whole email was a gigantic hyperlink, so if you clicked anywhere in the email, you would initiate the malicious attack.

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.

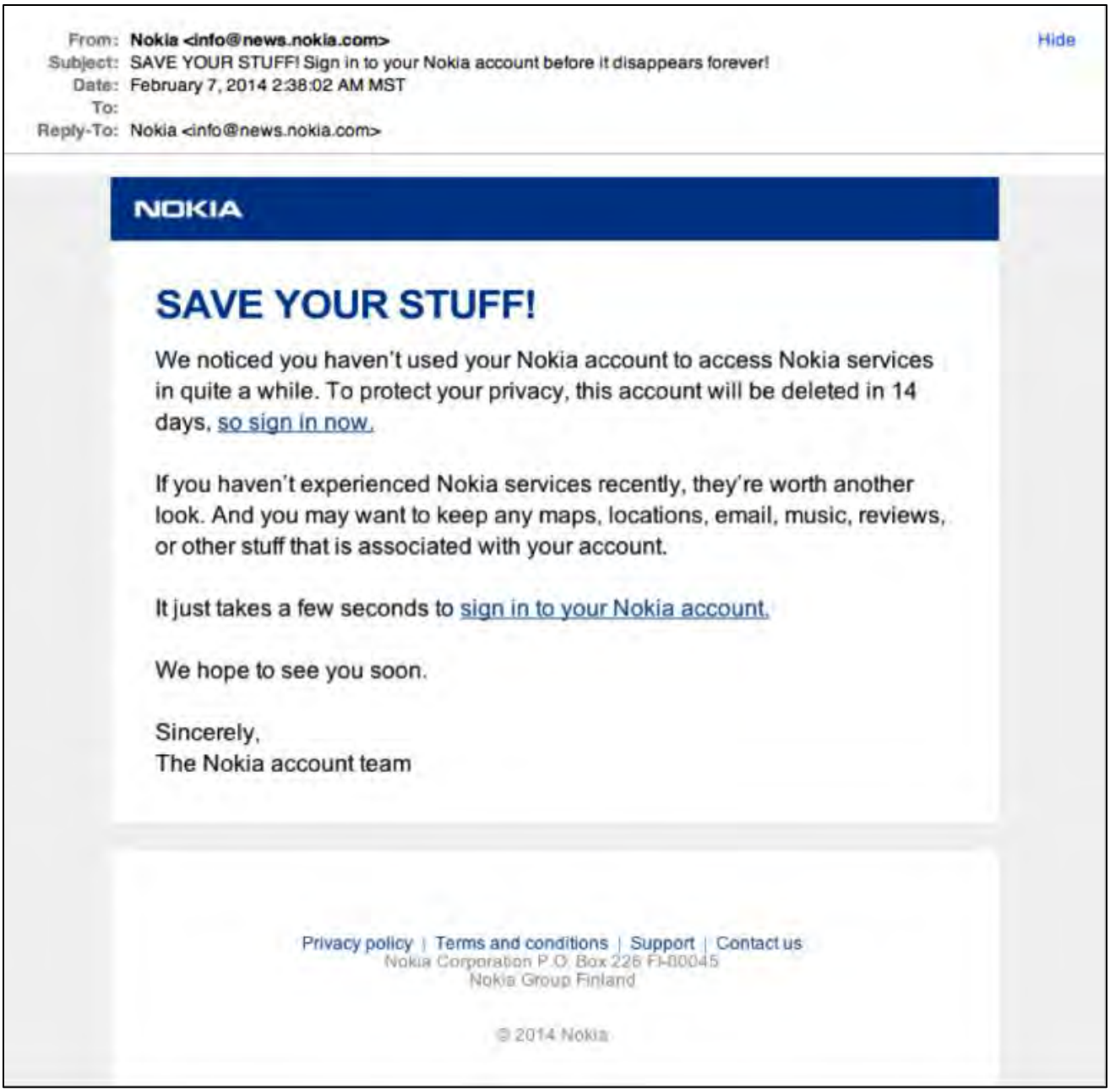
Like the tips above, this method isn't foolproof. Sometimes companies that already have your email will send you information, such as a white paper, that may require a download. In that case, be on the lookout for high-risk attachment file types include .exe, .scr, and .zip. (When in doubt, contact the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

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://.



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

It doesn't matter if you have the most secure security system in the world. It takes only one untrained employee to be fooled by a phishing attack and give away the data you've worked so hard to protect. Make sure both you and your employees understand the telltale signs of a phishing attempt.

David Ellis (GCIH, QSA, PFI, CISSP) is Director of Forensic Investigations at SecurityMetrics with over 25 years of law enforcement and investigative experience.

New Chapter Officers and Directors

We are pleased to announce the election of our slate of officers for the 2019-2020 Membership Year:

President:	Bobby Powell Holland Industrial, Henderson, NC
Vice President:	Billy Johns Stewart's Electric Motor Works Orlando, FL
Secretary-Treasurer:	Bill Henkel Rocky Mount Electric Motor LLC Rocky Mount NC

We are also glad to report that the following have been appointed as our new state directors:

Florida:	Todd Griffin Flanders Electric, Lakeland, FL
North Carolina:	Iain Jenkins Jenkins Electric, Charlotte NC
South Carolina:	Kelly Bolin Excel Apparatus, N. Charleston SC

More Bogus "Invoices" in Your Inbox

In the last issue of *Southwind* I mentioned that the old "Your Invoice is Attached" scam/spam/phishing email is going around, and it doesn't look like it will end anytime soon. I am still periodically hearing from members and friends who are receiving an email *supposedly* from the chapter that purports to have an invoice attached. I am also getting them *supposedly* from some of you, and I am getting "bounced" emails that I *supposedly* sent to invalid addresses. It is disgustingly easy for scammers, spammers and phishers to "spoof" someone else's email address, and it's maddening, but there's nothing much we can do about it. Inside this issue of *Southwind* is an article reprinted from securitymetrics.com that describes seven ways to identify phishing emails. I hope it will be helpful for our readers.

Remember: a good email rule is to *never* open any email attachment or click on any link inside an email unless you are sure that it is legitimate.

EASA Dues Season

One invoice that is not bogus is your EASA International dues invoice, and you should have it by now. Please remember that in accordance with EASA Governing Policy 20, the Southeastern Chapter will receive a ten-percent (10%) share of all dues paid up until February 28. Between March 1 and March 31 the chapter will receive a five-percent (5%) rebate. After March 31, the chapter will receive *no rebate*. The rebate on EASA International dues is an important part of the chapter's revenue and helps us provide the heavily subsidized training that is featured at our conferences. Thank you for helping us keep our chapter dues as low as possible by paying your International dues by February 28 if you can, but please not later than March 31.

EASA
The Electro-Mechanical Authority
SOUTHEASTERN CHAPTER
Raymond K. Paden, Executive Secretary-Treasurer
1395 Hampton Locust Grove Road
Locust Grove, GA 30248

rkpaden@easasoutheast.org
(678) 782-5961 FAX (888) 511-6336