I've Been Phished!

Corresponding Material
Digital Citizenship and Cyber Hygiene: Privacy and Security

Discussion
Phishing is a fraudulent attempt, usually made through email, to steal your personal information. The goal is to trick the email recipient into believing that the message is something they want or need so that they will click a link or download an attachment. Phishing is a play on the word "fishing", as it is a way of "throwing out bait" to see who bites. The best way to protect yourself from phishing is to learn how to recognize it.

How to identify phishing scams:

1. **Generic greeting -** Phishing emails are sent in large quantities in hopes that a percentage of recipients will not realize it is fraudulent. Do a quick check of how the sender addressed you!
2. **Generic body -** Phishing emails normally tend to have a generic body in the email. By keeping the information nonspecific, the internet criminals hope that the user believes that at least some of the information applies to them. Take a quick moment to assess whether the information is actually about you!
3. **Incorrect Company Information -** Many phishing emails do not send the email from an email address with the correct domain (i.e. from the correct company). Some sender emails will try to trick you by having the correct subdomain, but not the correct domain (i.e. @am.amazon.com instead of @amazon.com)
4. **Request for personal information -** Companies do not request personal information over email since it email is insecure. If an email is asking for personal information, it is most likely a phishing email.
5. **Sense of urgency -** Internet criminals want to get your personal information now so they can move on to another victim. To do this, phishing emails normally make you think that something needs to happen fast to fix the situation. If an email is asking you to act fast, don't! Slow down and assess the situation.
6. **Poor grammar -** Internet criminals are not dumb. They prey on the uneducated because they are easier targets. An email from a legitimate organization should be well written. Any email with poor grammar should be enough to cause you to pause and evaluate the email.
7. **Still can't tell?** Call the company and ask!

I've been phished! Now what?

- Do not click on any links or open attachments.
- Do not reply to the sender.
- Report the scam (forward the email to the FTC - spam@uce.gov)
- If you do legitimate business with the spoofed company, you may inform the company of the phishing email in circulation.
- Delete the email.

Uh oh. I fell for a phish! What now?

- Don't panic!
- Change passwords to any website you have logged into since the phish.
- Scan your computer for viruses.
- Contact the company who has been spoofed so they can alert other people!
- If this happened on a school computer, let an administrator know as soon as possible.

Class Exercise

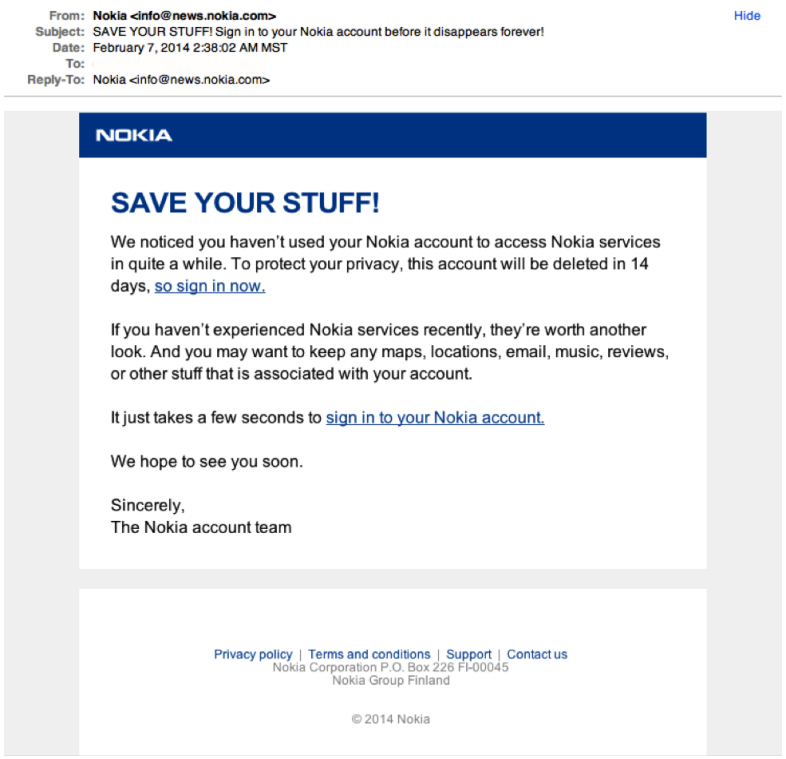
Observe the following real-world phishing examples. For each example, explain how you can tell that it is a fraudulent email.

Example:

Notes:

- Generic greeting - This email has a generic greeting and does not address the recipient by name.
- Incorrect company information - This email address is missing an "A", so is clearly not from an Amazon employee. Also, the link reveals that it points to a non-Amazon site, which should not be the case if this was a legitimate email from Amazon.
- Sense of urgency - The email is stating that the user needs to click a link in the next 36 hours or else their Amazon account will be terminated.
- Poor grammar - The grammar in this email is not professional. The misspelling of "believe" should be a red flag.

Email #1:



From: Nokia <info@news.nokia.com> Hide
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>

NOKIA

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.

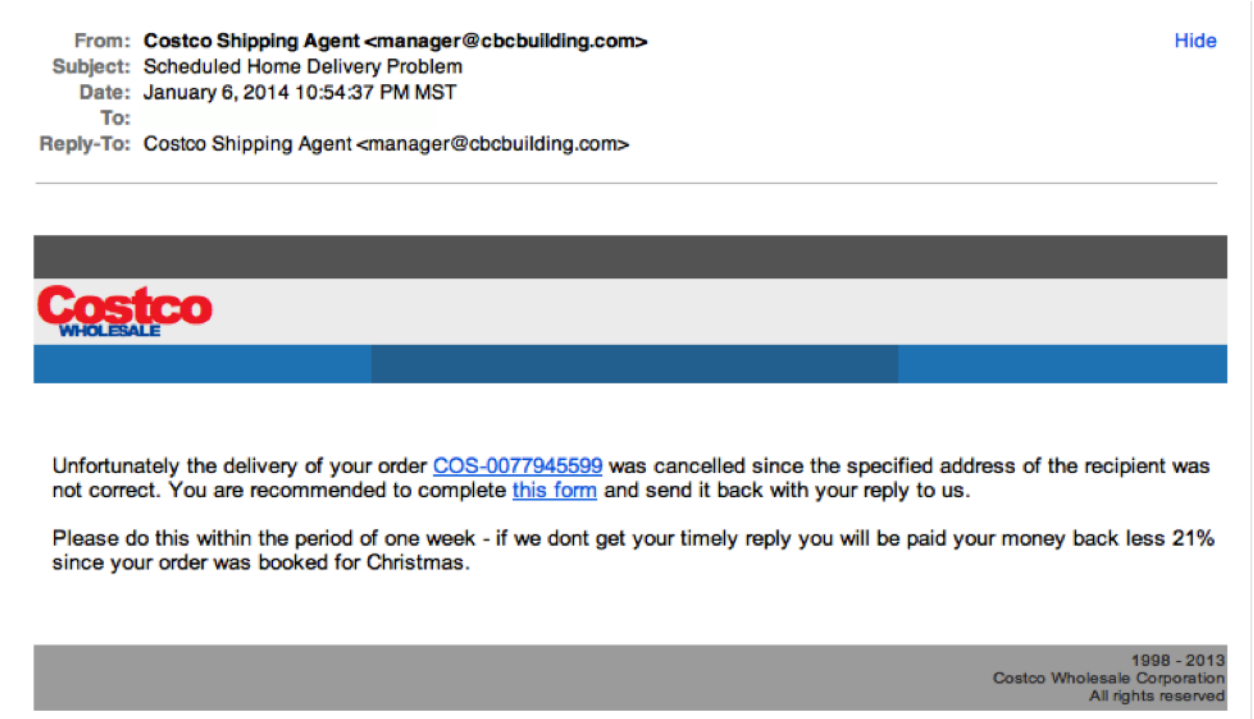
Sincerely,
The Nokia account team

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

© 2014 Nokia

Notes:

Email #2:



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.

Notes:

Email #3:

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

Notes: