



The Ultimate Five-Minute Guide to Cyber Security for Your Business

**Fact: It's not a matter of *if*
you'll get hacked,
but *when*.**

**The best defense against
a cyber threat is staying
up to date with cyber
news and best practices.**

These slides will show you exactly how to identify and avoid a threat, and what to do if you experience one.

What are four common
cyber security risks?

1

Clicking on spam emails



Careless internet browsing



Poorly constructed passwords

4

Software that's
misconfigured or
outdated

Let's start with
spam emails...

Email Threats

Hackers can gain access to your confidential information through email.

Email Threats

Email threats are
commonly identified as...

Phishing

Spear Phishing

Spoofing

Phishing

Spear Phishing

Spoofing

Phishing emails are designed to make you click a corrupted link to download malicious software that cripples your devices or steals your information.

Common signs of a phishing email:

- » Misspelled words or poor phrasing
 - » Phony email address
 - » Phony URL
 - » Request for action

Phishing

Spear Phishing

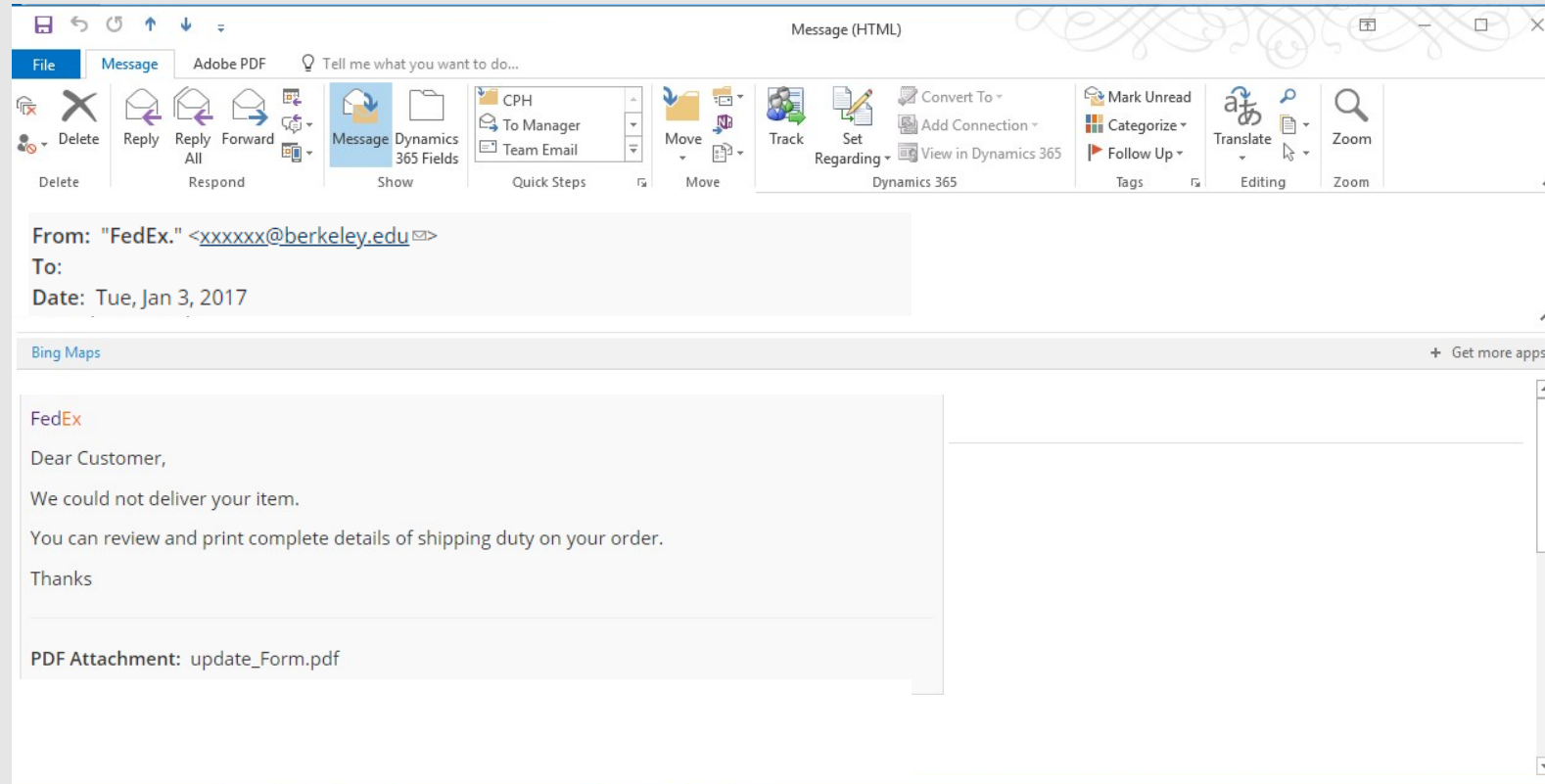
Spoofing

Can you spot the red flags in
this example?

Phishing

Spear Phishing

Spoofing

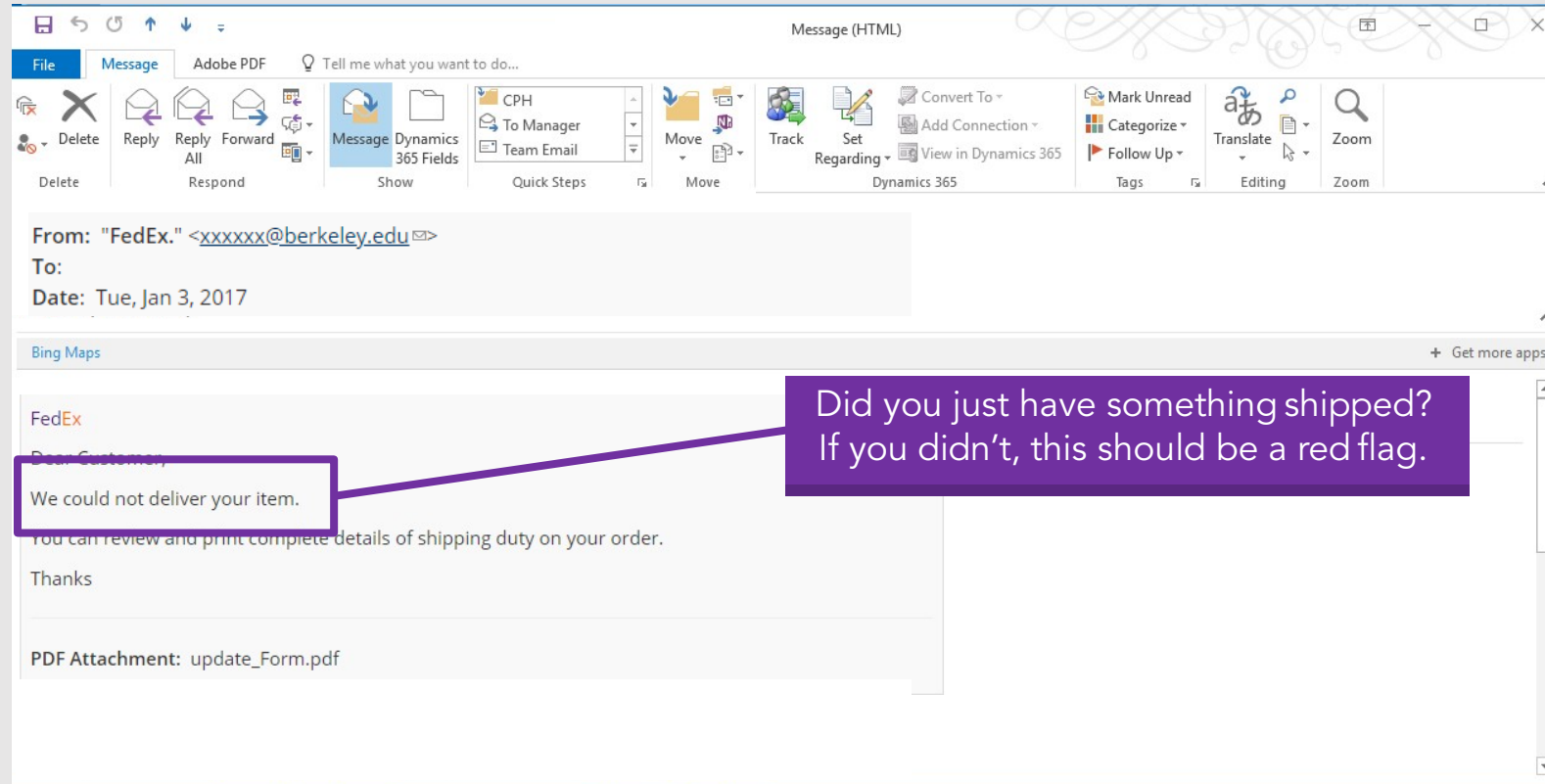


<https://security.berkeley.edu/news/phishing-example-fedex-shipment-update>

Phishing

Spear Phishing

Spoofing

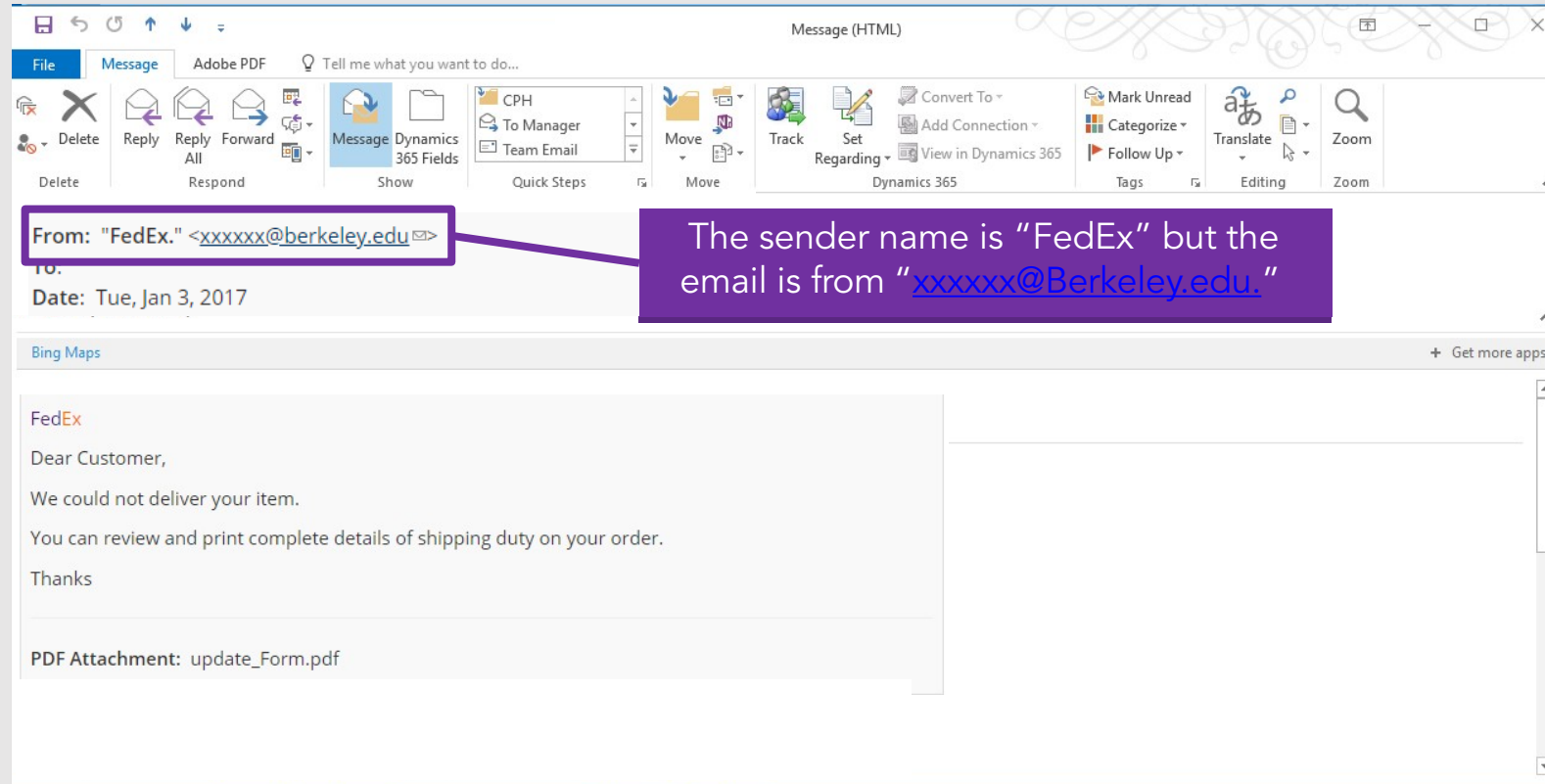


<https://security.berkeley.edu/news/phishing-example-fedex-shipment-update>

Phishing

Spear Phishing

Spoofing

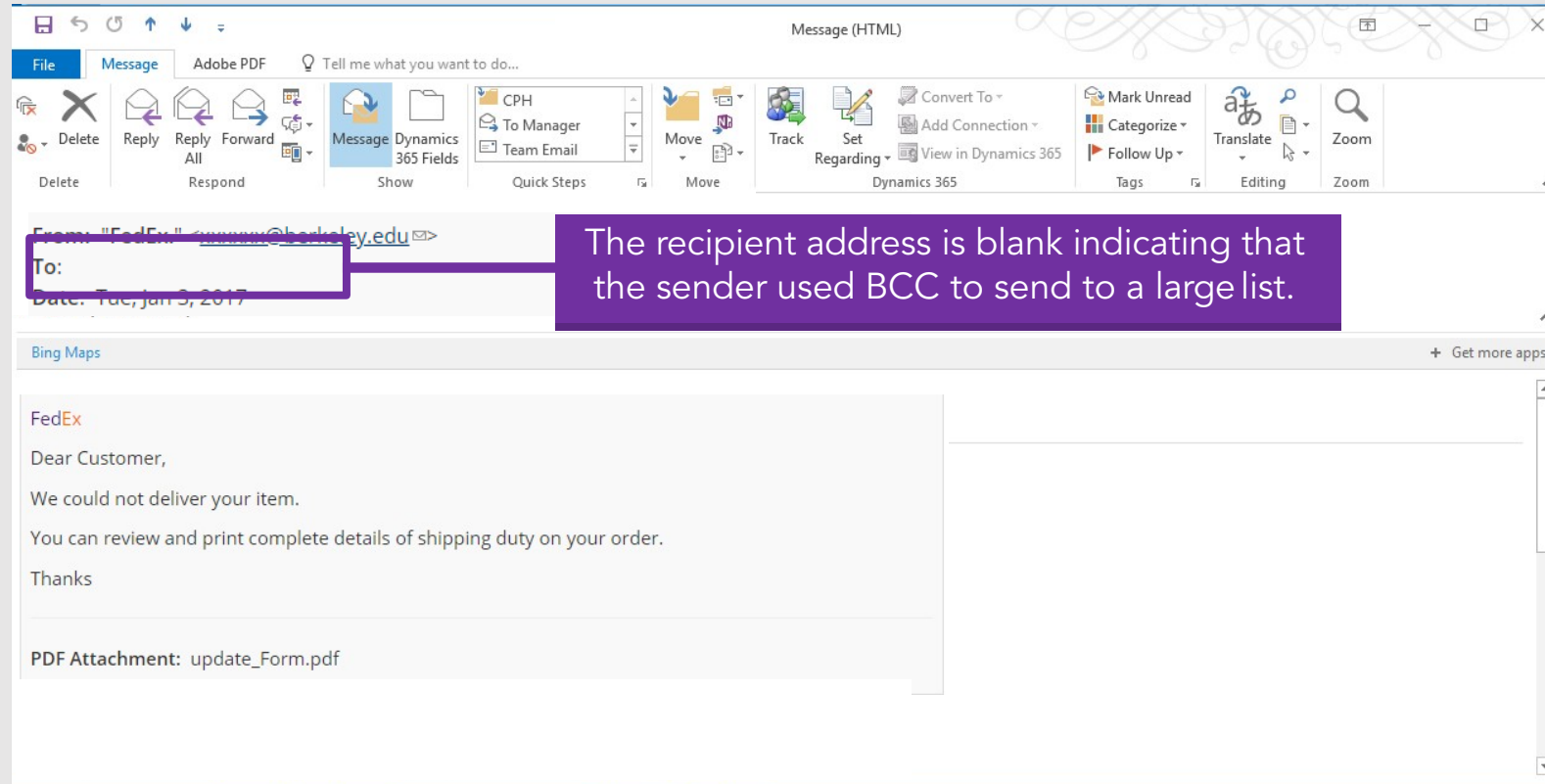


<https://security.berkeley.edu/news/phishing-example-fedex-shipment-update>

Phishing

Spear Phishing

Spoofing

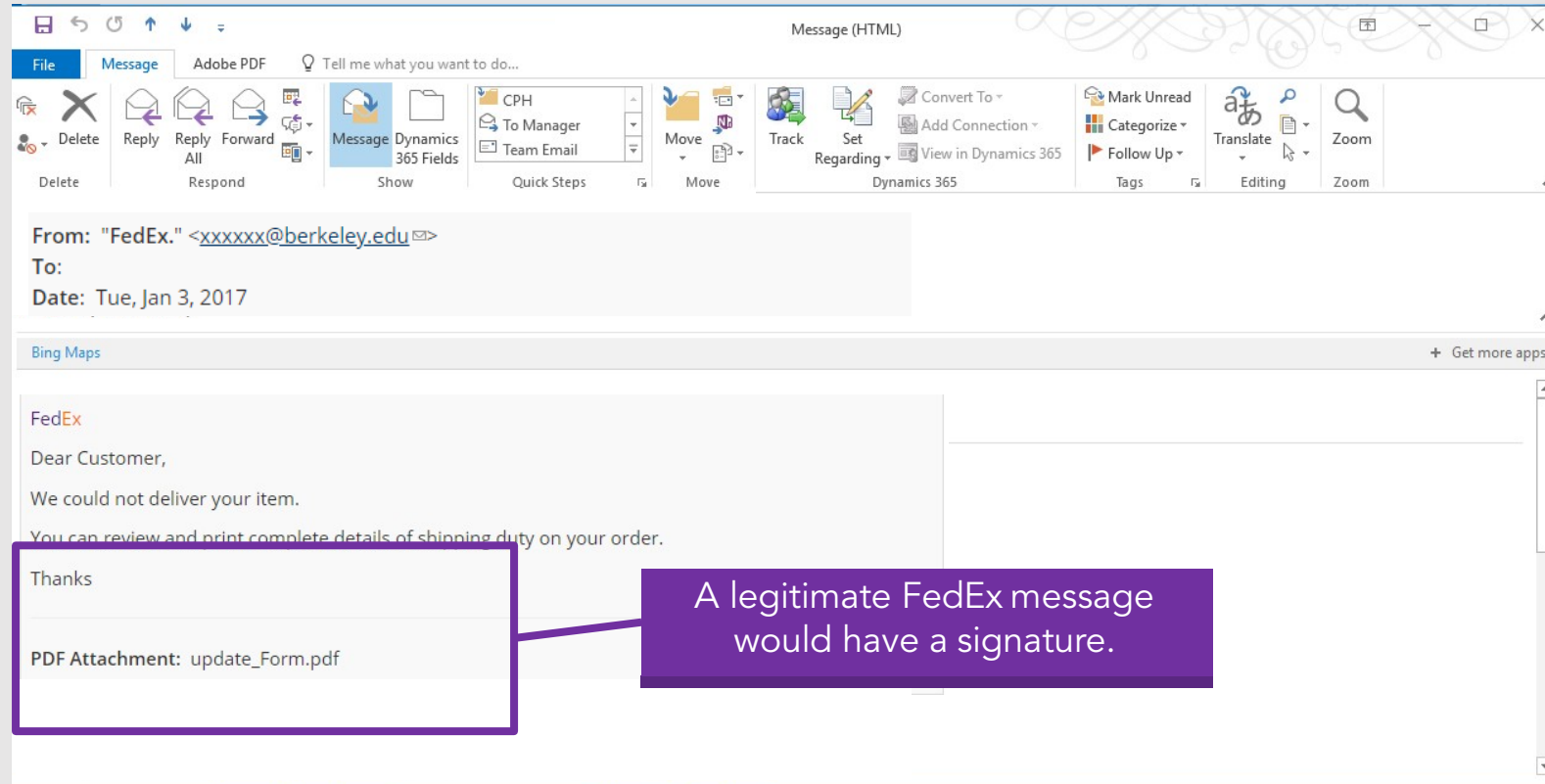


<https://security.berkeley.edu/news/phishing-example-fedex-shipment-update>

Phishing

Spear Phishing

Spoofing

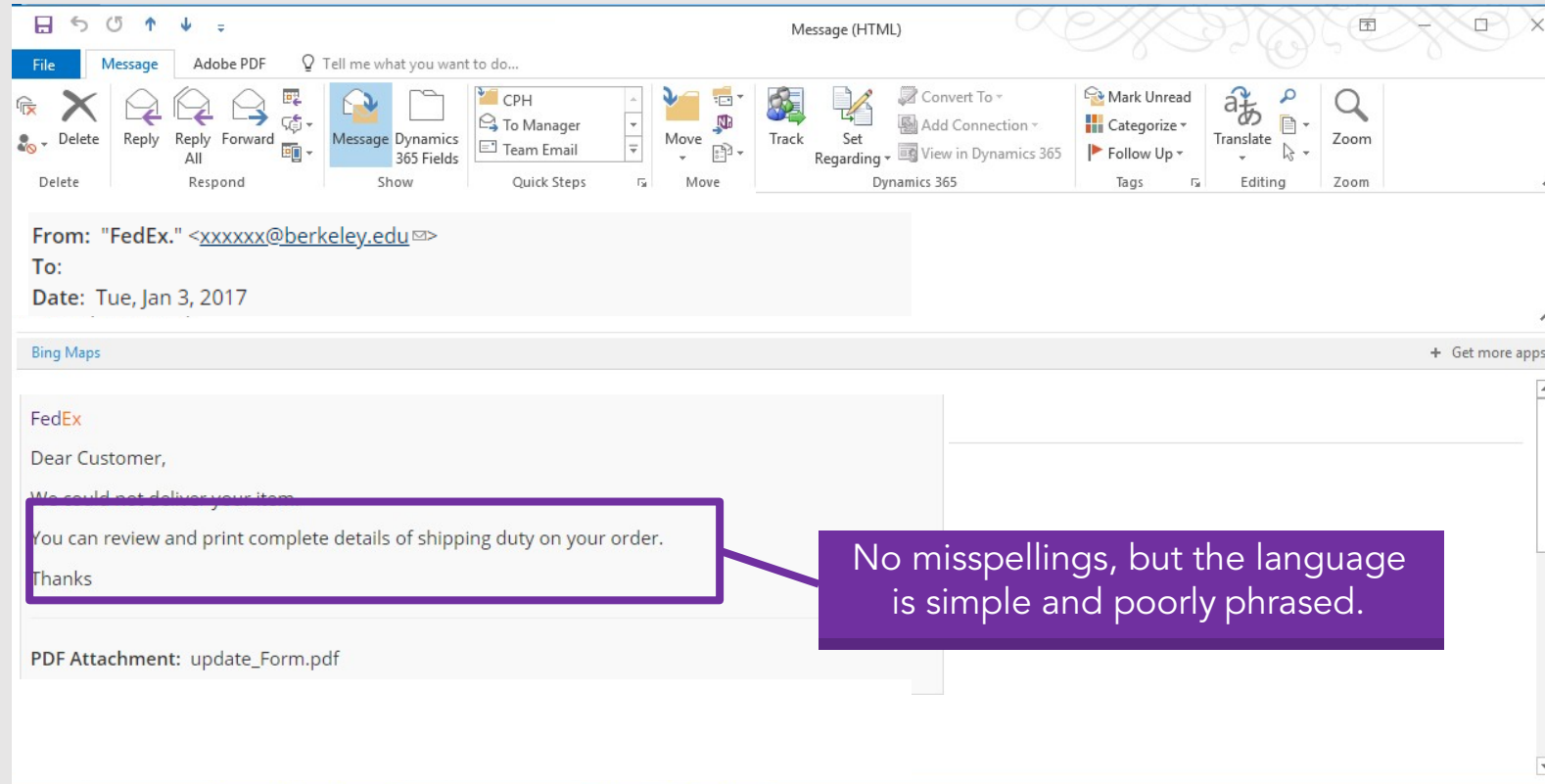


<https://security.berkeley.edu/news/phishing-example-fedex-shipment-update>

Phishing

Spear Phishing

Spoofing



<https://security.berkeley.edu/news/phishing-example-fedex-shipment-update>

Phishing

Spear Phishing

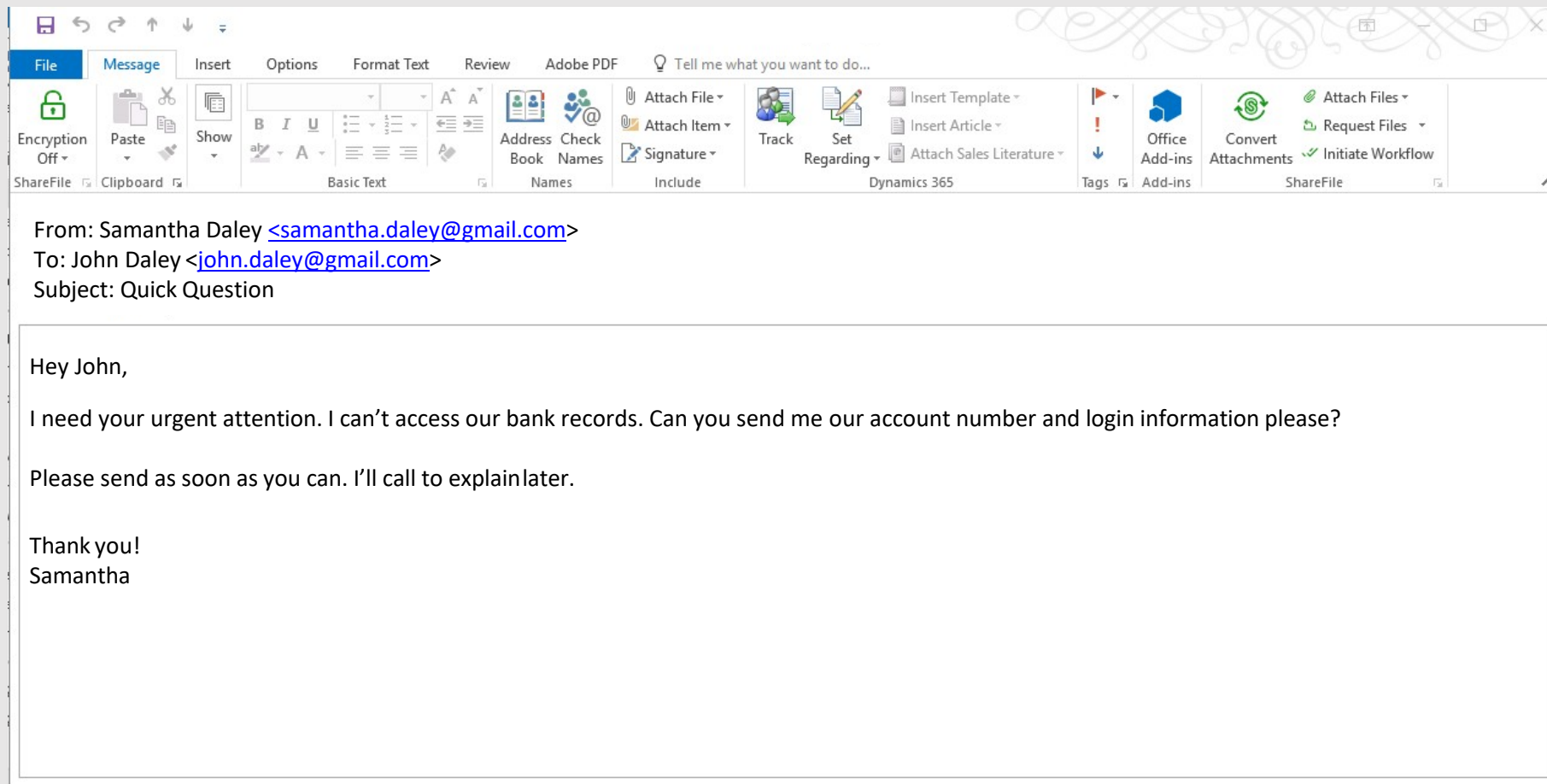
Spoofing

Spear phishing is a more sophisticated form of phishing. It still requests that the recipient downloads a file or clicks on a link, but **the sender looks like someone you know.**

Phishing

Spear Phishing

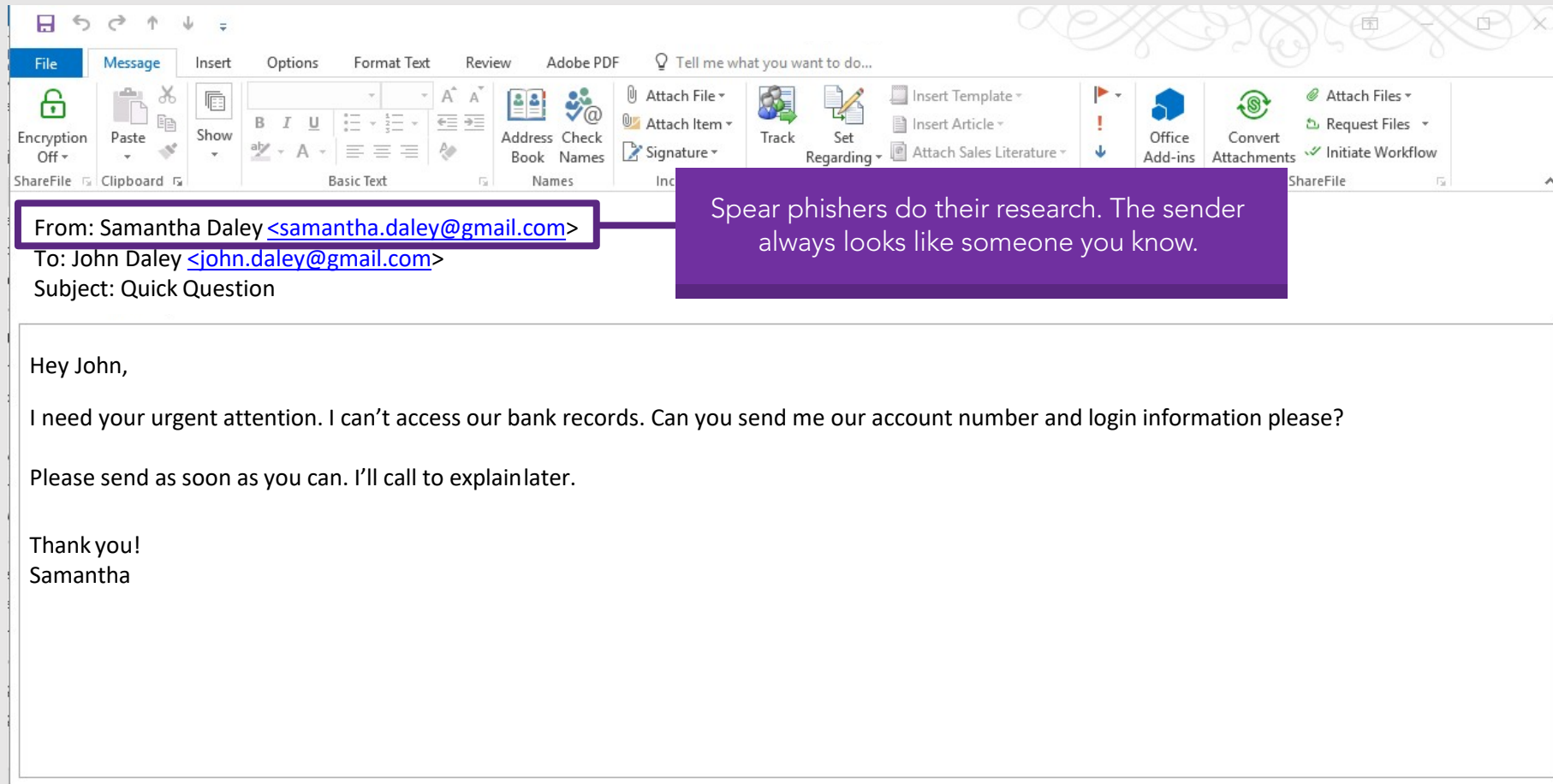
Spoofing



Phishing

Spear Phishing

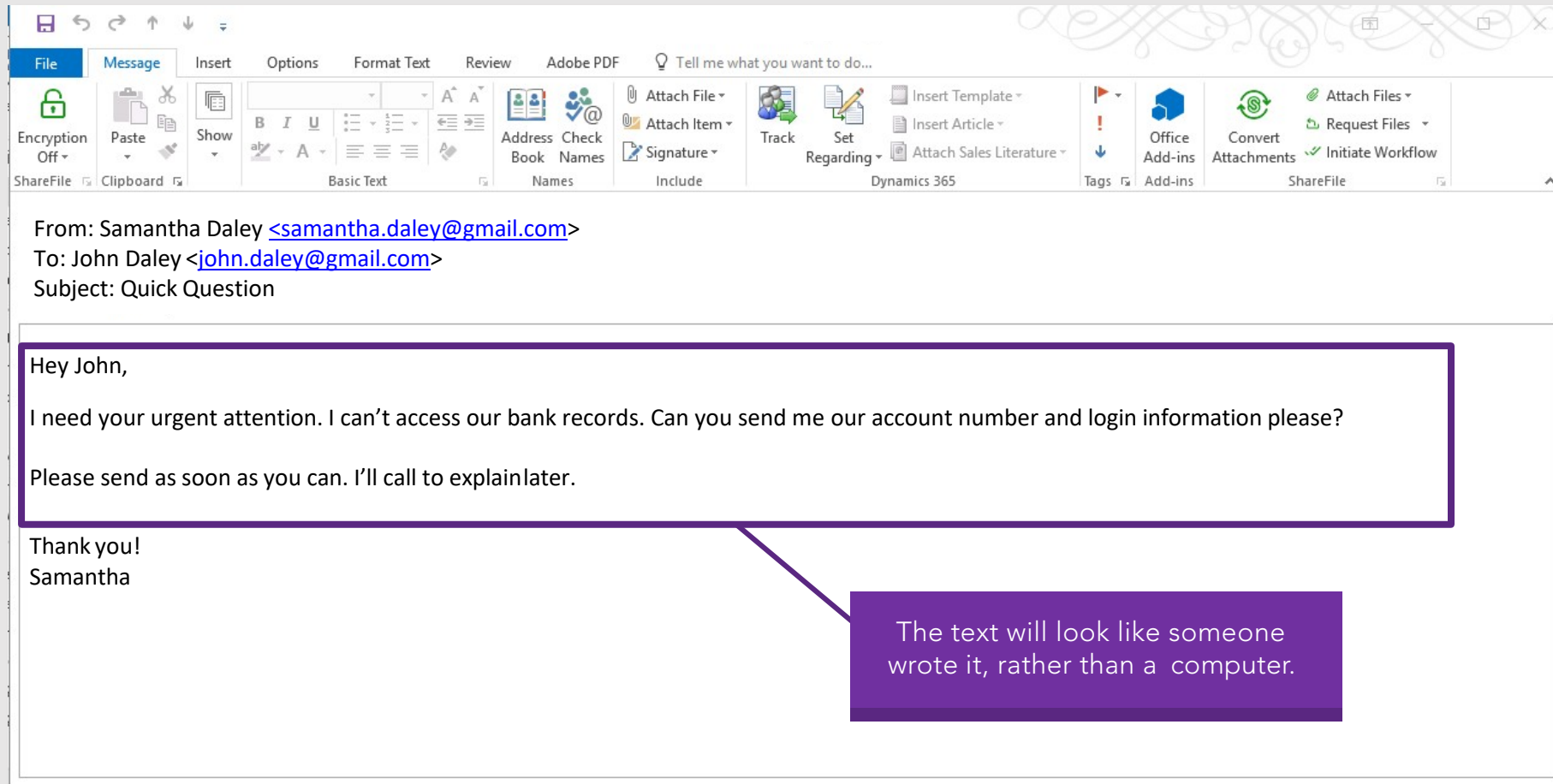
Spoofing



Phishing

Spear Phishing

Spoofing



Phishing

Spear Phishing

Spoofing

So how do you know it's a spear phishing scam?

Phishing

Spear Phishing

Spoofing

1. They demand an urgent action that would require sharing confidential information or a wire transfer.

Phishing

Spear Phishing

Spoofing

2. They ask something that the real sender would not likely ask of you.

Phishing

Spear Phishing

Spoofing

If you suspect the sender is a spear phisher, call the sender to confirm that they really sent it.

Phishing

Spear Phishing

Spoofing

Spoofing is the act of disguising a fake email address with a real one.

Phishing

Spear Phishing

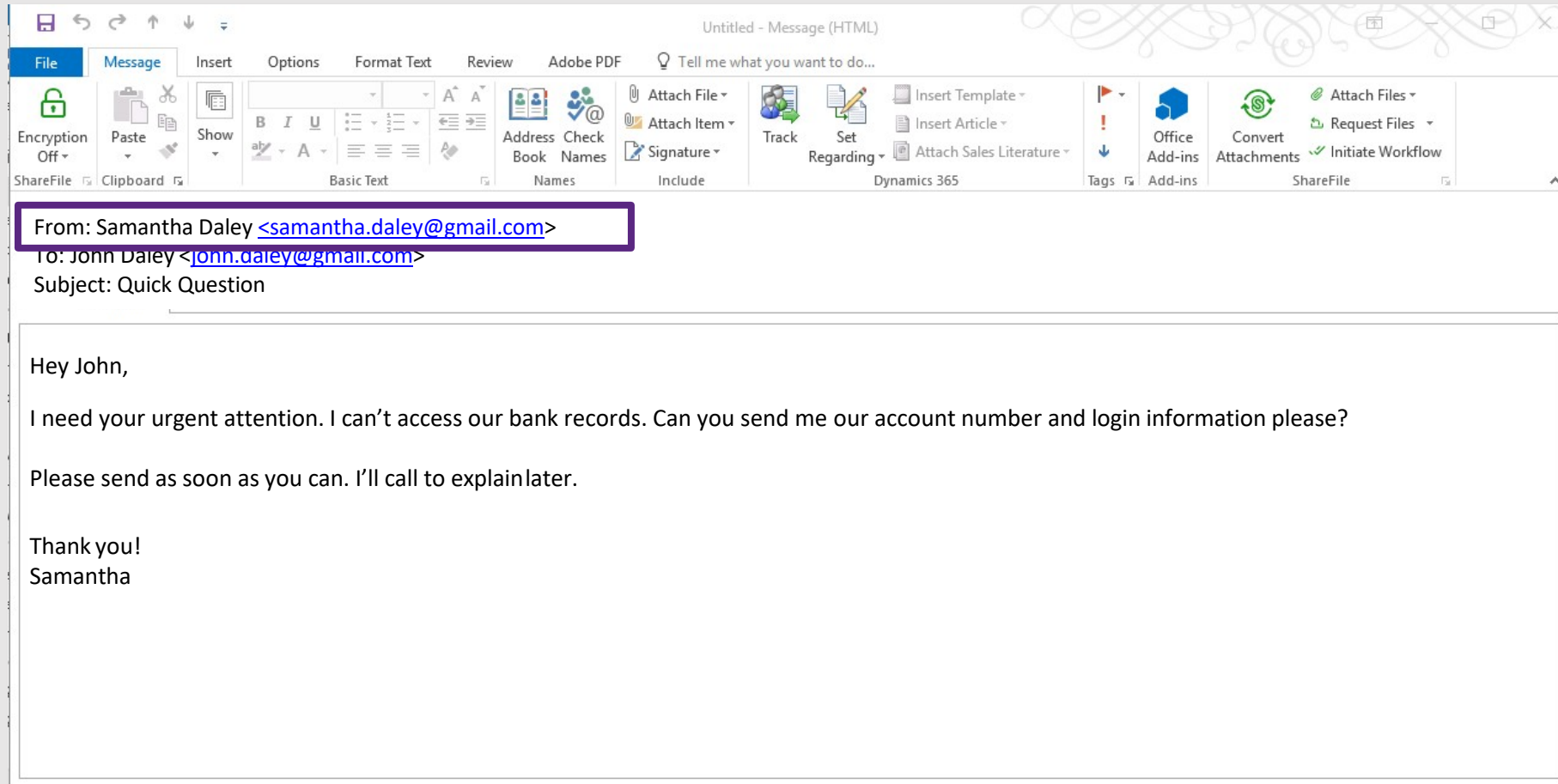
Spooofing

So an email shows up in
your inbox and the sender
looks like this...

Phishing

Spear Phishing

Spoofing



Phishing

Spear Phishing

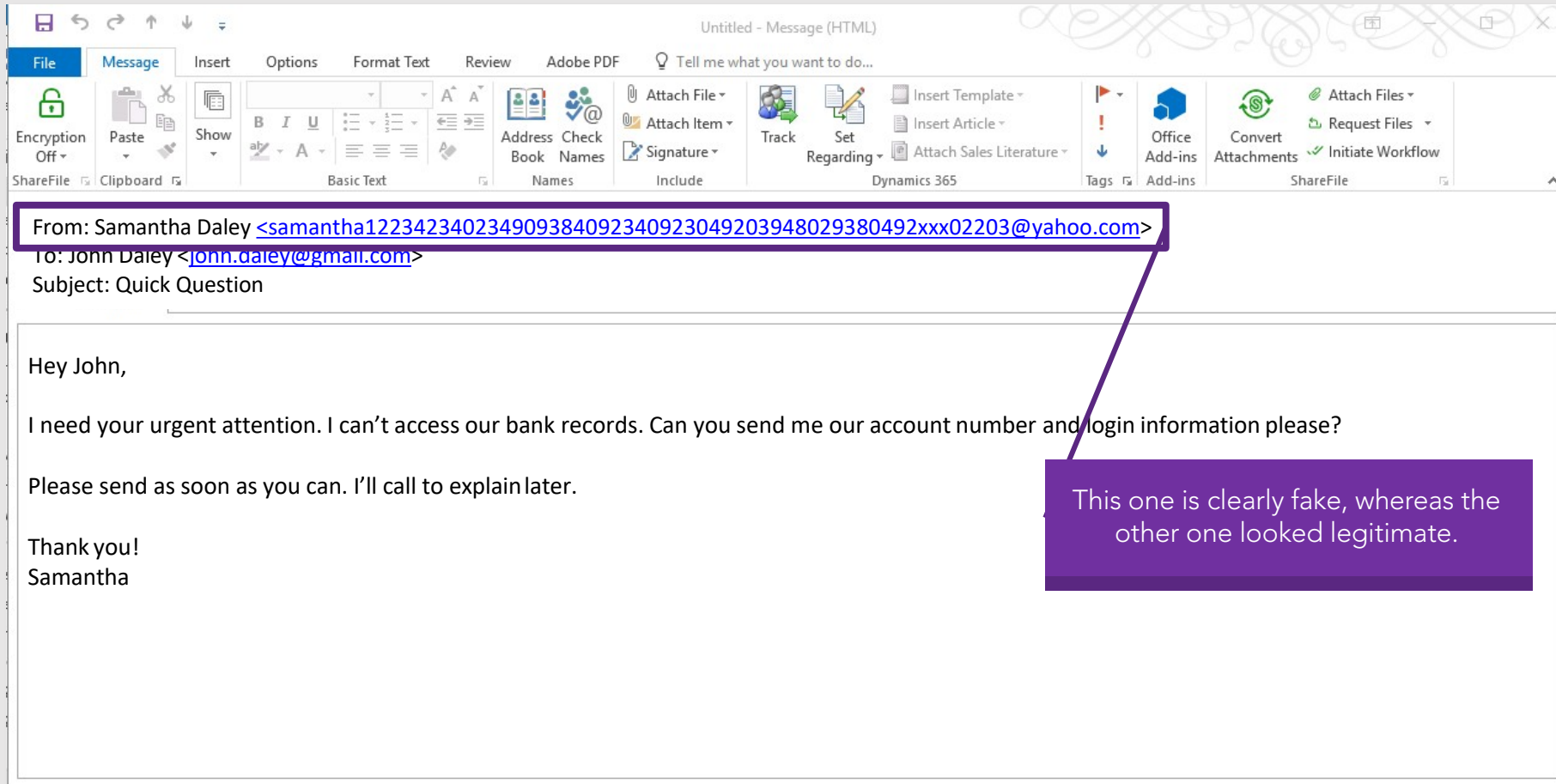
Spoofing

Rather than this...

Phishing

Spear Phishing

Spoofing



Phishing

Spear Phishing

Spoofing

Spoofers use mail workarounds to make it look like a legitimate email source.

Phishing

Spear Phishing

Spoofing

This puts the recipient's guard down and entices them to give in to the spoofer's demands.

Email Threats

The only way to avoid being a victim of a phishing, spear phishing or spoofing hack is **to think before you click.**

Email Threats

If you recognize the signs, delete the email and alert IT support team (if you have one).

Internet Threats

Clicking on the wrong website can cause a slew of security issues as well.

Internet Threats

This could result in harmful spyware or malware being installed on your computer.

Internet Threats

Browse on websites that start with https:// rather than http:// to ensure you have a secure connection.

Ransomware 101

Let's discuss this notorious threat...

Ransomware 101

Ransomware is a malicious software that holds your data for ransom. It downloads to your computer, cuts off access to your data, and demands that you pay a certain amount of money to restore it.

Ransomware 101

It can get into your computer through unprotected websites, spam emails and more.

Ransomware 101

Here's what it looks like when it takes over...

Wanna Decryptor 1.0

Ooops, your files have been encrypted!



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

About bitcoin
How to buy bitcoins?

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

QR Code
Copy

<http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034>

What do you do if you
get a ransomware
message?

Step 1

Unplug your computer immediately. This stops malware from spreading to other devices.

Step 1

Step 2

Alert your IT
support team.

Step 1

Step 2

Step 3

Keep calm and let
your IT support
handle the rest.

How do you protect yourself from cyber threats?

Update Your Security Software

This includes enabling two-factor authentication and checking to make sure notifications are being sent to the right place.

Update Your Workstation

Keep up on your operating system and workstation updates. They'll protect you from known vulnerabilities.

Switch Up Your Password

Password safety standards say you should be using phrases rather than words in your passwords.


Stay Alert To New Threats

Then share them with your employees and coworkers they don't make a costly mistake.

Contact Our Team

 Bill Walter, MCP, MCSE, PMP

 wwalter@gma-cpa.com

 443.610.7413



GROSSMENDELSON

ACCOUNTING • TECHNOLOGY • WEALTH ADVISORY