WINE INDUSTRY

TECHNOLOGY

SYMPOSIUM

Gone Phishing:
Practical Steps to Protect Your Business

Charles Tango – CISO, Altria

WITS

October 1, 2019
CIA @ Copia, Napa, CA

Why am I here?

I love wine!

No, really

Charles is the **Chief Information Security Officer at Altria**, the parent company of producers of superior branded tobacco and wine products such as Philip Morris USA and **Ste. Michelle Wine Estates.**

Charles also represents Altria on **the board of the Richmond Technology Council**, which supports technology innovation in the greater Richmond area, as well as the **board of the Virginia Cybersecurity Partnership**—a joint information sharing organization between government agencies and the private sector. Additionally he is a member of **IBM Security's Advisory Board** and holds advisory board positions with two tech start-ups.

Prior to his role at Altria, Charles held senior level Information Security positions with financial institutions in the NY metro area, including Chief Information Security & Risk Officer for Sterling National Bank and Senior Vice President, IT & Operational Risk at Citigroup.

The basics

What is phishing?

What is phishing?

phish·ing: a method of trying to gather personal information using deceptive e-mails and websites.

/ˈfiSHiNG/
noun

Spear Phishing	*Very targeted phishing, often designed for a specific user*
Vishing	*Phishing over the phone*
Smishing	*Phishing via SMS (text message)*
Search Engine Phishing	*A fake webpage that shows up in a search due to keywords*
Whaling	*Spear Phishing that targets C level or VIP*

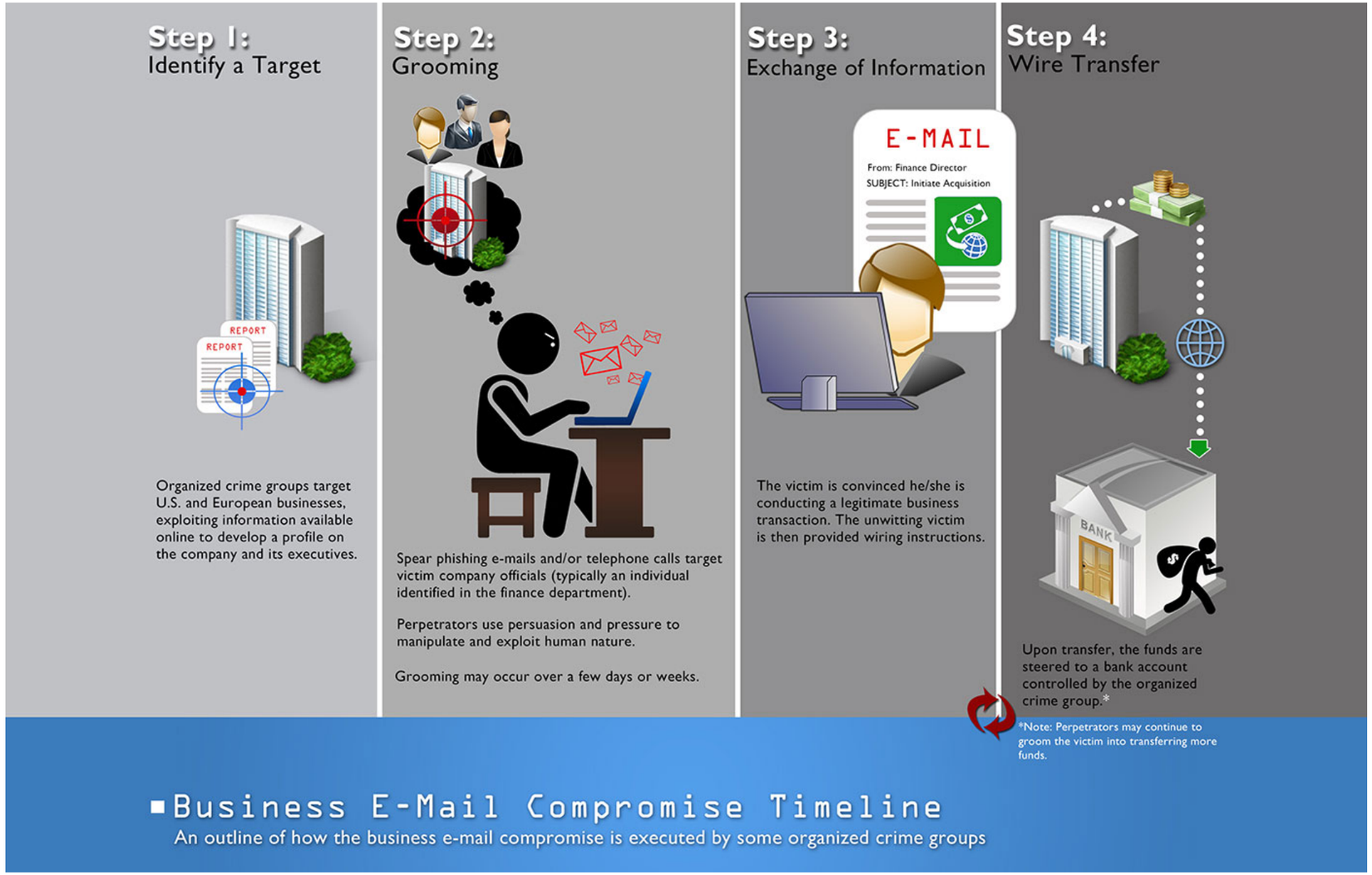
It’s a big deal

- Phishing is the #1 cause of data breaches -- and has been for a while

- Other types of attacks steal the headlines but don’t lead to data breaches as often
- Stolen credentials are the #2 cause of data breaches -- guess where they get those credentials
- Other notable attacks are tied to phishing, such as malware and Business E-mail Compromise (BEC)

*all stats as per Verizon Data Breach Report and CSO Magazine

What about BEC?

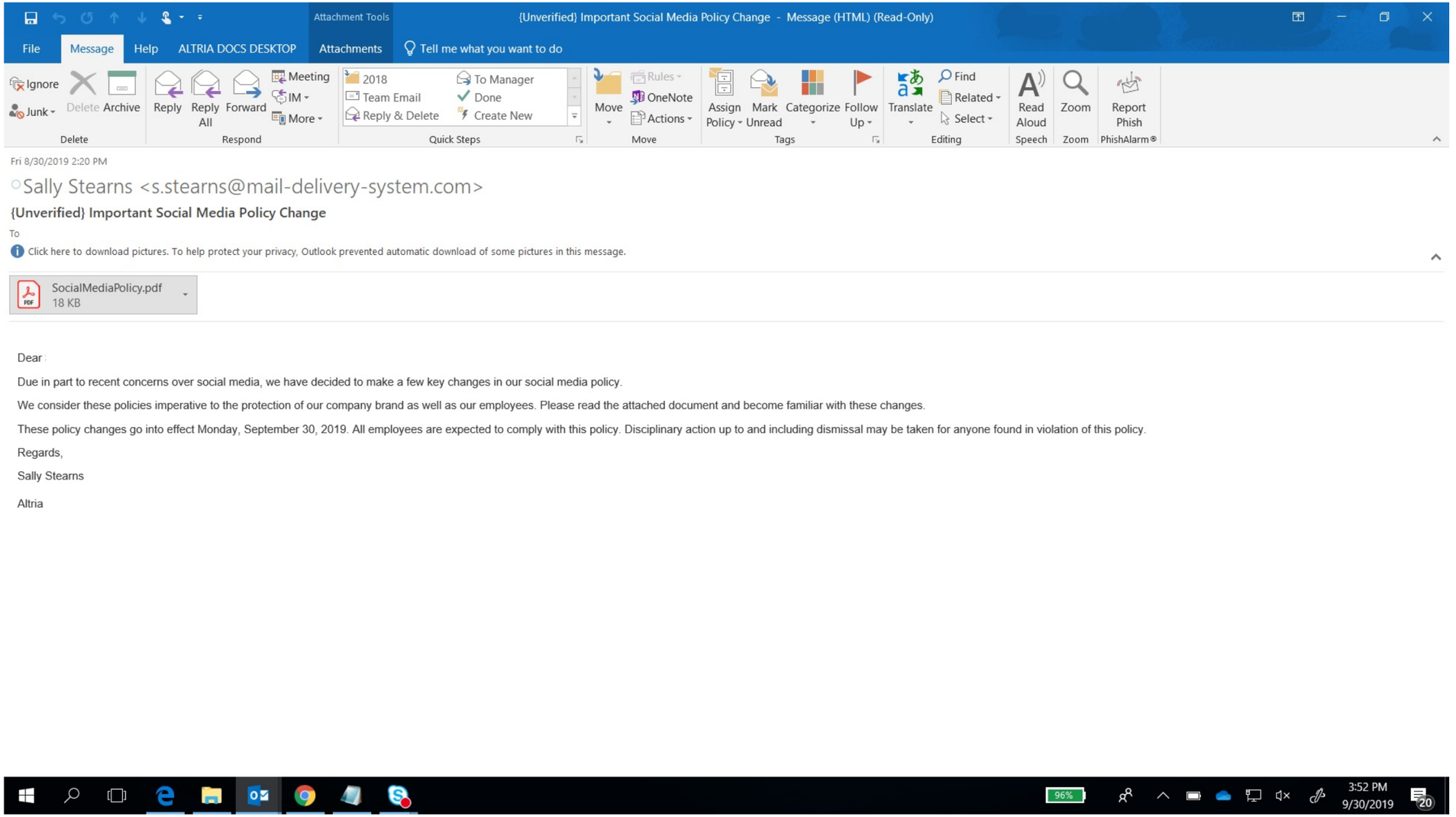


According to the FBI, global **BEC attacks** led to over **$1.2 Billion in losses across the US in 2018** – up by over 100% from 2017

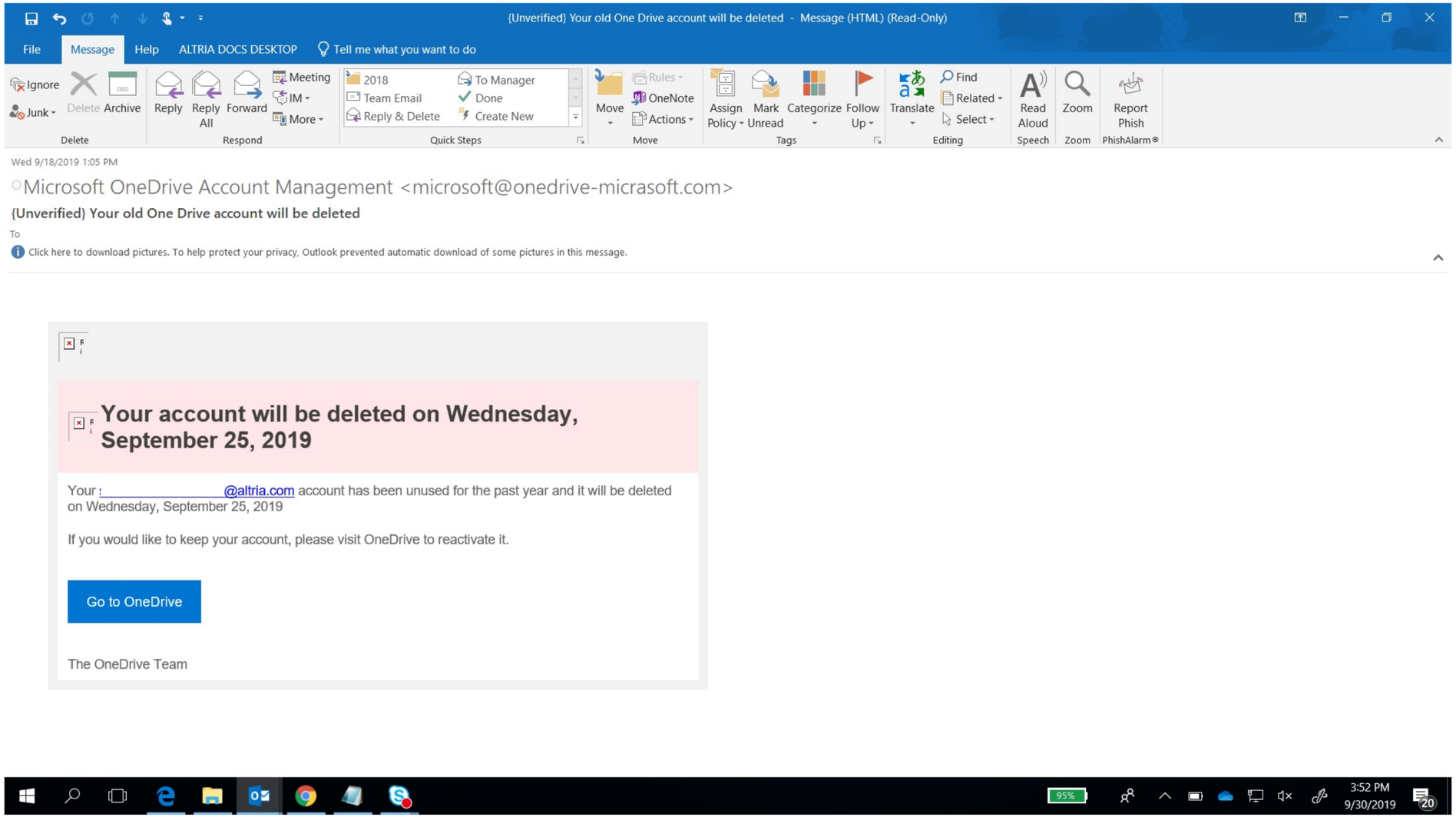
The 2018 **BEC average loss** was **$64,000**

**all stats and image as per FBI and IC3 report*

Phishing Example



Phishing Example 2



How to prevent a successful phish

People are the first line of defense

- There’s no technology that can stop all phishing, so ultimately its up to your people
- Perform simulated phishing tests
- Make it easy for employees to report suspected phishing – and reward them for doing so
- Teach them how to spot a phish
- …. and don’t forget to train your IT department on how to respond

Hackers go email phishing with lures to tempt you.

Here are some things to keep in mind before you click, so you don't get caught by an email hook.

P opular company logos and content are used for a sense of familiarity to lure you in to a feeling of complacency.

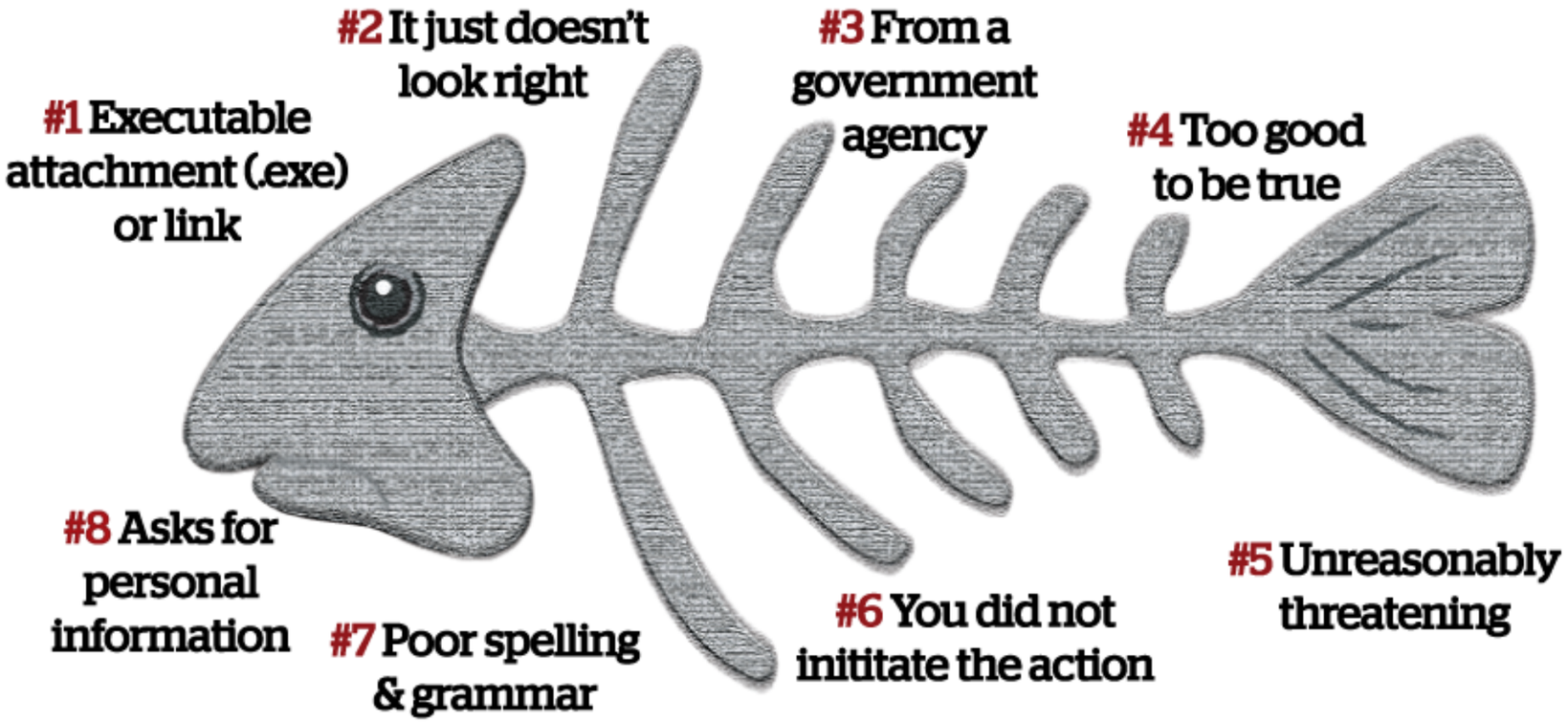
H TTP is not secure, HTTPS is not guaranteed. Your own internet search of the web address will help you know if it's legit.

I ndirect threats or scare tactics may be used, such as "A*ct now or your account will be disabled*."

S pelling is frequently bad and the grammar may be poor as legitimate companies rarely make errors.

H over your mouse before you click and determine where a link in the email points of if it's an executable (.exe) file.

Eight Signs of a Phish



Learn the signs: Don't get hooked by phishing.

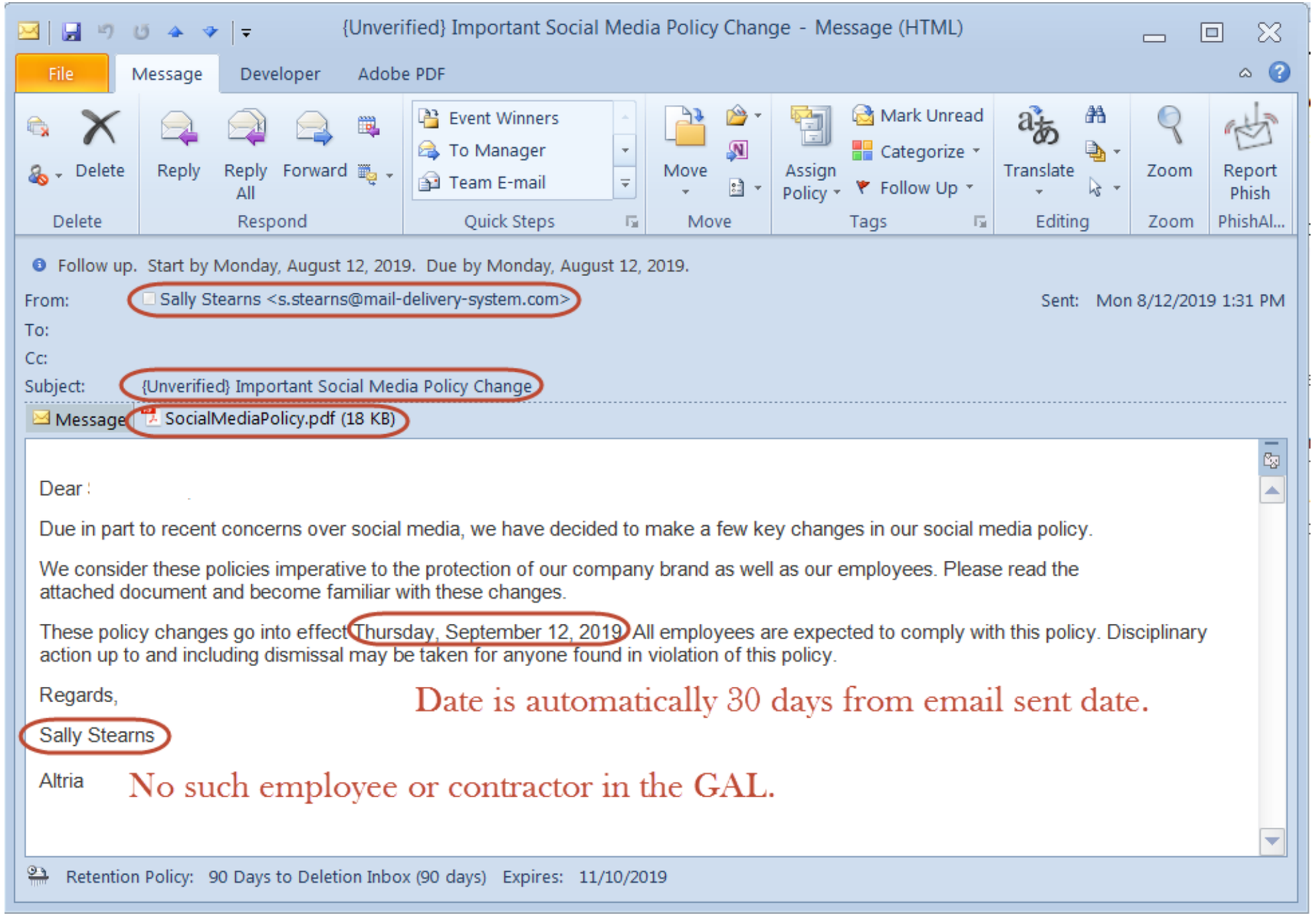
Technology can help

- There are a number of phish detection services which work with most e-mail providers
- Inbound e-mail can be tagged in the subject line to make it obvious to the user it came from the outside
- One-click solutions exist which make it easy for users to report a suspected phish
- Utilize web proxy software which can block malicious sites if a user does click on a link
- And of course, make sure you have appropriate anti-malware for both your e-mail systems and end users

Let’s put that to use

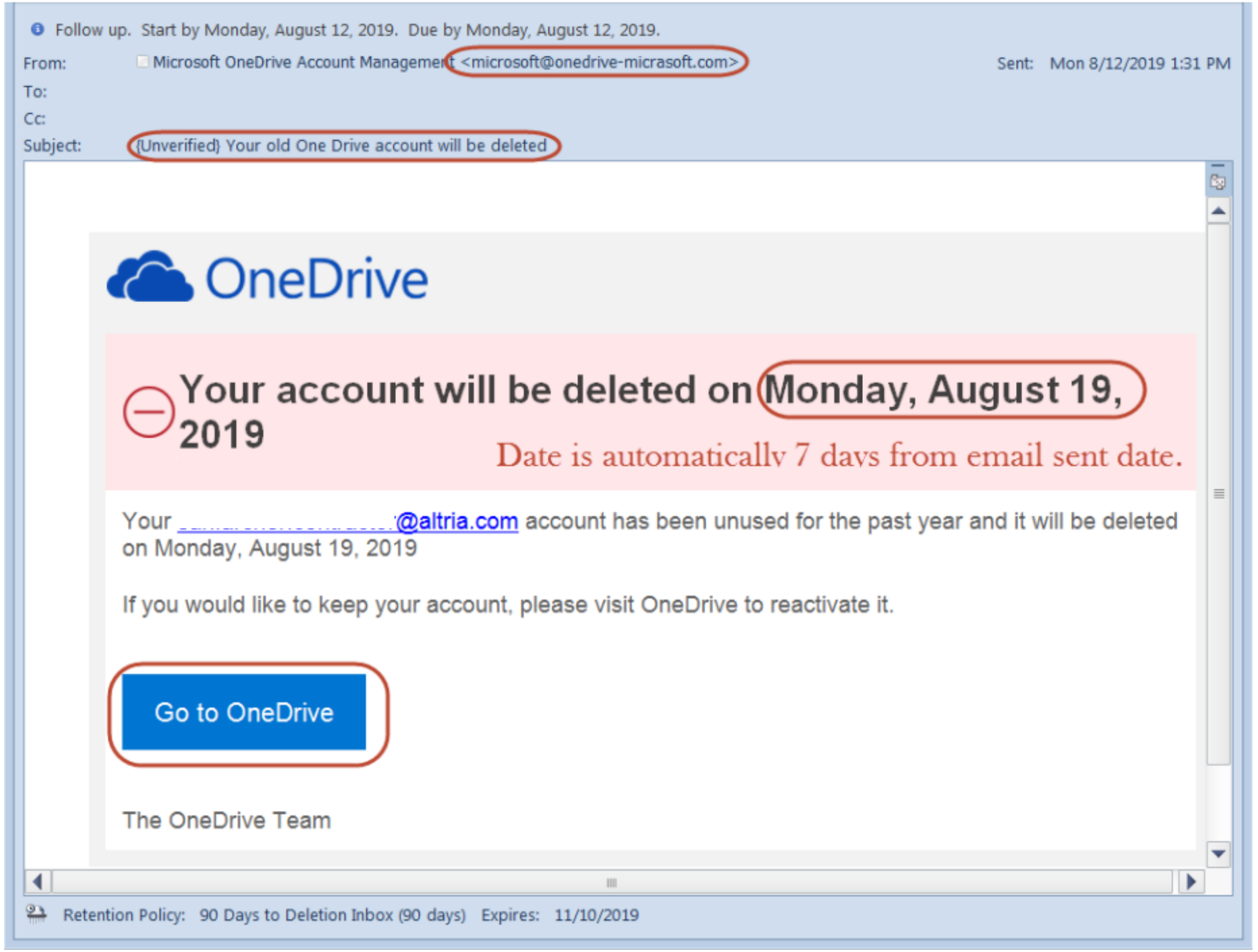
Example 1 Revisited

- Suspicious “from” address
- Sender is external even though they pretend not to be
- Unexpected PDF attachment
- Date set with forceful language for non-compliance
- Sender is non existent



Example 2 Revisited

- Fake Microsoft “from” address
- Sender is external even though they pretend not to be
- Date set with forceful language for non-compliance
- Link which does not go to OneDrive when moused over



You can prevent BEC, too

- First and foremost, make sure your financial processes (e.g. wire transfer) have multiple controls to prevent fraudulent transactions

- Configure your e-mail so that when accessed externally it requires two-factor authentication

- Work with your IT department to implement technical changes which reduce the likelihood of someone spoofing or intercepting your e-mail
  - DMARC & SPF – Helps prevent spoofing of e-mail addresses
  - TLS – Encrypts e-mail between sender and recipient

What happens if

You fall for a phish

- Stay calm – but act quickly
- Notify your IT and/or Security department and follow their lead
- If you **are** IT:
  - Force the user's password to be changed
  - Block the sender address and any malicious links that were included in the phish
  - Scan the machine for malware
  - Identify and remove other copies of the same phish other users have received
  - Look for unauthorized or suspicious activity on your systems
  - If you suspect a broader issue, or if you are in over your head, bring in an expert

Recap

Recap

- Phishing is the largest source of data breaches and can lead to BEC, which will cost you money
- Phishing comes in many forms, not just e-mail
- Employees are the first, and last line of defense. Awareness and training are key
- Technology can help your employees be successful
- Work with your IT and Security departments to prevent these risks. Retain external security services in the event you have an issue
- When in doubt, ask an expert. We're everywhere

Questions and Contact

charles.tango@altria.com

c.f.tango@gmail.com

https://www.linkedin.com/in/charles-tango-27856117/