E-MAIL SECURITY MITIGATION

EMAIL IS A TOP THREAT VECTOR

Data breaches have become one of today's biggest business threats. In the U.S. alone, companies and government agencies suffered a record 1,093 data breaches last year. That's a 40% increase from the year before, according to the Identify Theft Resource Center.

The top threat vector for those data breaches: email. According to Verizon, email fraud accounts for 95% of enterprise attacks.

95%

of enterprise attacks are email fraud

Today's Email Security Tools Are Failing

There's a 22% chance that any given organization will experience a data breach of at least 10,000 records within the next 24 hours.

Source: Proofpoint

Only 31% of companies have a budget in place for data breach mitigation.

Source: Osterman Research

75% of organizations would take hours, days or weeks to detect a breach.

Source: Osterman Research

The Problem

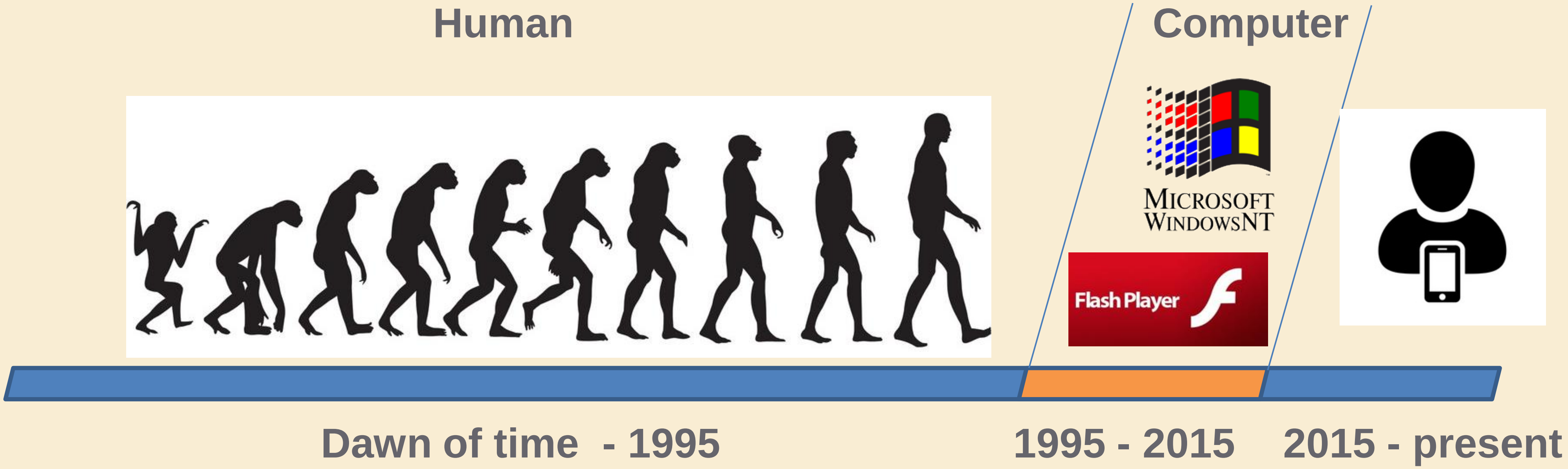
ATTACKS ARE EVOLVING FASTER THAN EMAIL DEFENSES

Since its inception, email has been a favorite target for cyber criminals hoping to steal sensitive data, user credentials, and company funds. In response, organizations have deployed a wide range of email security tools. Most of these focused on protecting the network.

But attack techniques are evolving fast. Solutions built for fighting the attacks of two to three years ago are struggling to keep up. For example, business email compromise (BEC) email fraud was barely on the radar 24 months ago. Now, it has eclipsed ransomware in terms of monetary loss.

Amid dramatic headlines and more aggressive regulation, organizations are expected to spend more than $90 billion on cybersecurity in 2019. That's a huge disconnect. Organizations are spending more on cybersecurity than ever, even as losses from data breaches, business disruption and fraud continue to mount.

Who is Easiest to Fool?



Human

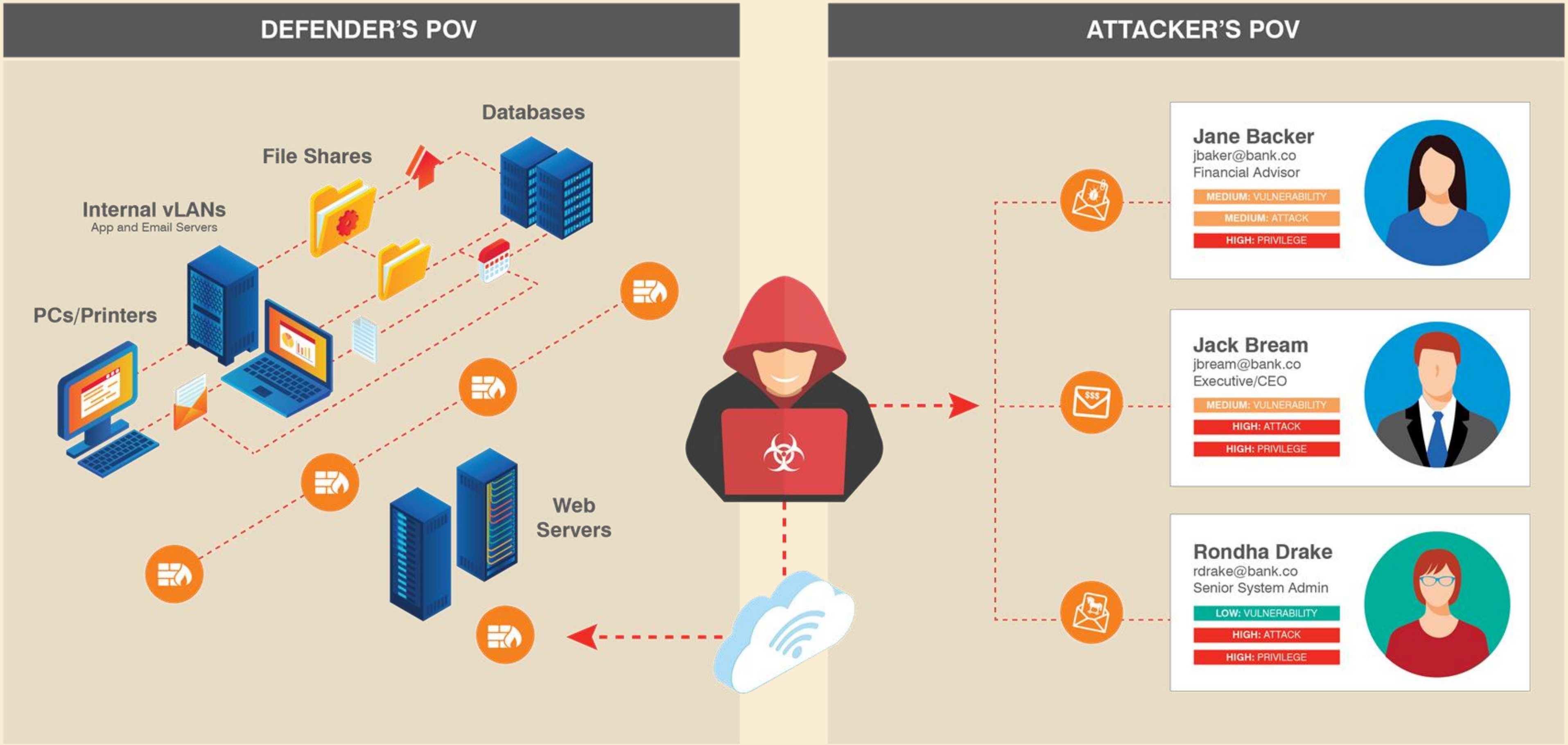
Computer

Dawn of time - 1995

1995 - 2015

2015 - present

Defensive strategy needs to rival attacker tactics



DEFENDER'S POV

ATTACKER'S POV

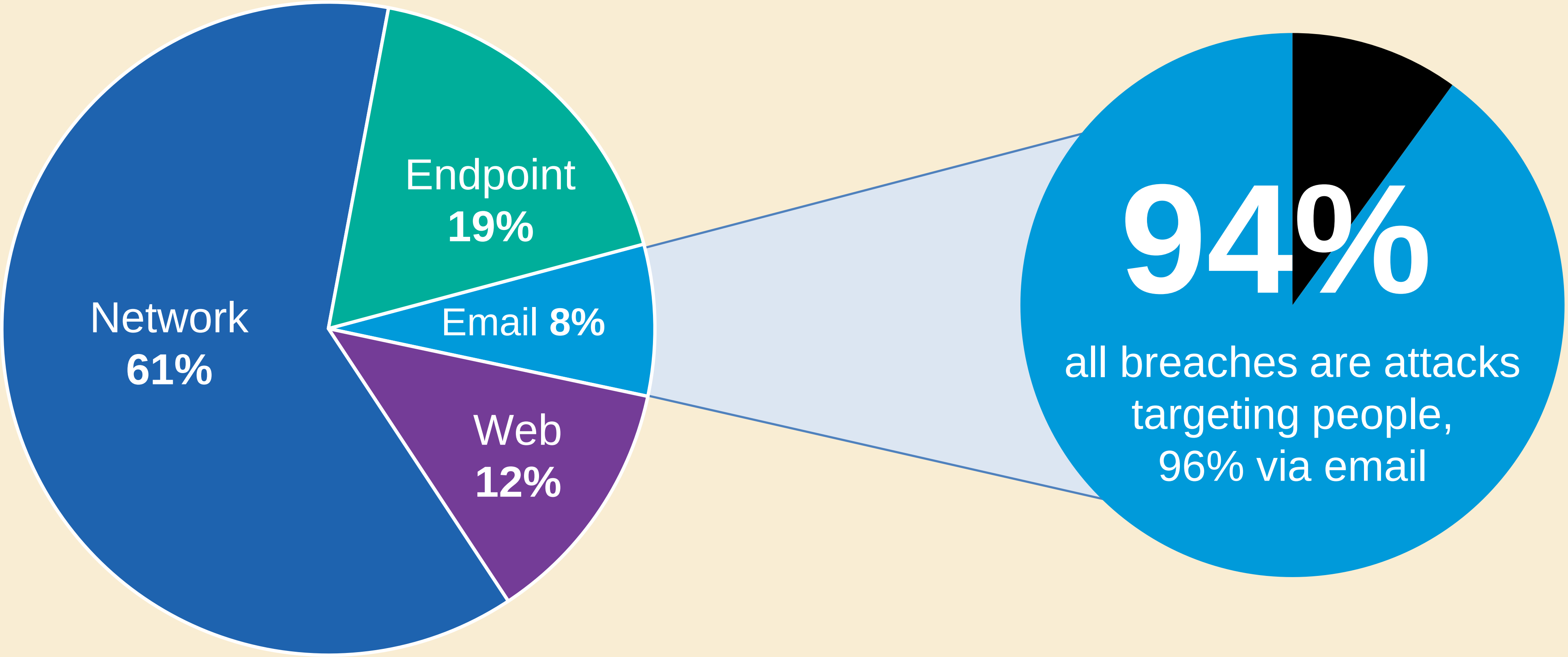
Jane Backer
jbaker@bank.co
Financial Advisor
MEDIUM: VULNERABILITY
MEDIUM: ATTACK
HIGH: PRIVILEGE

Jack Bream
jbream@bank.co
Executive/CEO
MEDIUM: VULNERABILITY
HIGH: ATTACK
HIGH: PRIVILEGE

Rondha Drake
rdrake@bank.co
Senior System Admin
LOW: VULNERABILITY
HIGH: ATTACK
HIGH: PRIVILEGE

Defenders don't focus on people, attackers do

Security Spending



Source: Gartner Information Security, Worldwide 2016 – 2022, 1Q 2018 update (2018 forecast)

Attack Vectors

94%

all breaches are attacks targeting people, 96% via email

Source: 2018 Verizon DBIR

Today’s Top Email Fraud Tactics

Cyber criminals use a wide range of tactics to launch email attacks.

- Account Compromise
- Credential Phishing
- Impersonation
- Advanced Malware
- Outbound Phishing

1. Spoofing Email Fields

Spoofing email fields is a popular BEC tactic. Attackers have several ways of doing this, including:

❑ Changing the reply-to email address

❑ Spoofing the display name

❑ Using use a domain that looks like the company's but is slightly different

❑ Pretending to be a legitimate business partner or supplier

2. Targeting a Range of People

❑ President
❑ Students
❑ Teachers
❑ Employees

3. Getting Creative with Subject Lines

Using "clickbait" subject lines is another favorite tactic. Urgent language is the most popular—employees are more likely to pay attention to a fraudulent reply-to address if the subject line suggests that someone in authority needs something from them.

Most Popular BEC Subject Lines

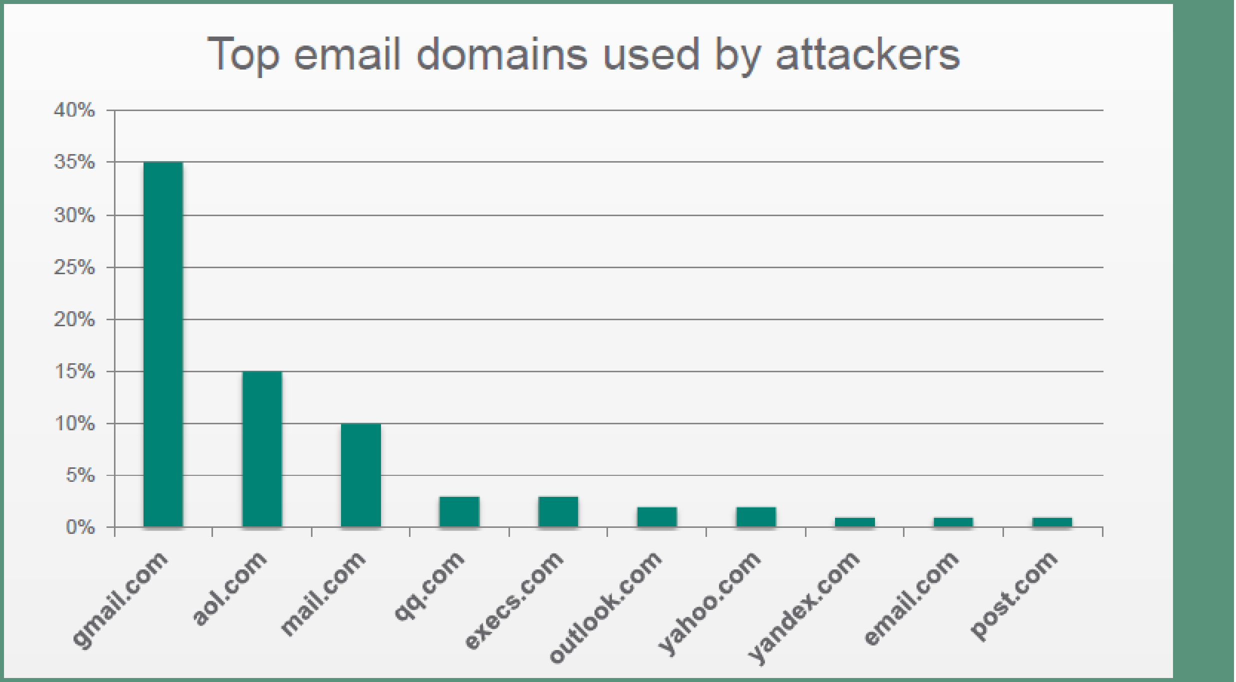
- Payment
- Request
- Urgent

Top email subject categories

❑ Payment
❑ Request
❑ Urgent

Top strings in spoofed email addresses

❑ ‘ceo’ -<ceo@fakedomain.com>
❑ ‘exec’ -<exec@fakedomain.org>
❑ ‘office’ -<office@baddomain.net>



4 STEPS TO BUILDING YOUR EMAIL SECURITY STRATEGY

Step 1: Authentication

Step 2: Content Inspection

DMARC ensures that legitimate email is properly authenticating and that fraudulent activity appearing to come from your organization's domains is blocked

You Need Authentication and Content Inspection

Passport Control

1 We need to put a greater emphasis on senders being able to prove that they are who they say they are

2 While continuing to ensure that content is screened and behaviors are monitored

Step 3: End User Training

Introduce interactive user awareness training

"Teachable moments" are powerful – use to your advantage

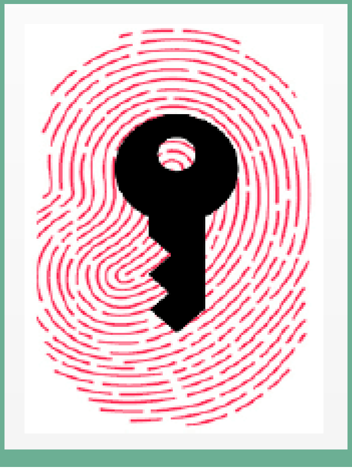
Up to 90% reduction in successful external phishing attacks and malware infections with Wombat Security

Step 4: Strong Authentication for Approvals

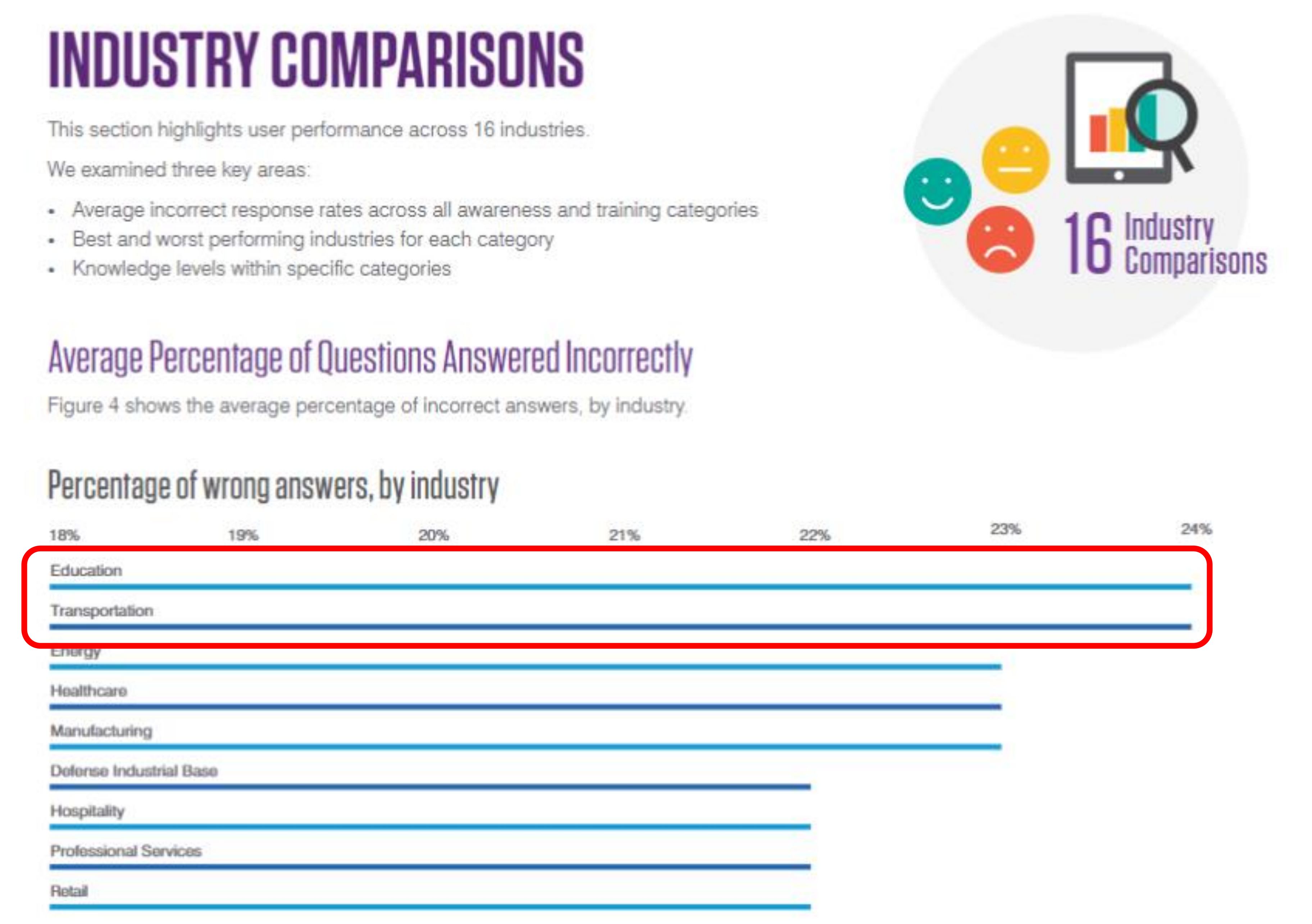
- No single person authorization

- Written approvals critical business functions (e.g. financial transactions)

- Multi-factor authentication



Something in common



INDUSTRY COMPARISONS

This section highlights user performance across 16 industries.

We examined three key areas:

- Average incorrect response rates across all awareness and training categories
- Best and worst performing industries for each category
- Knowledge levels within specific categories

16 Industry Comparisons

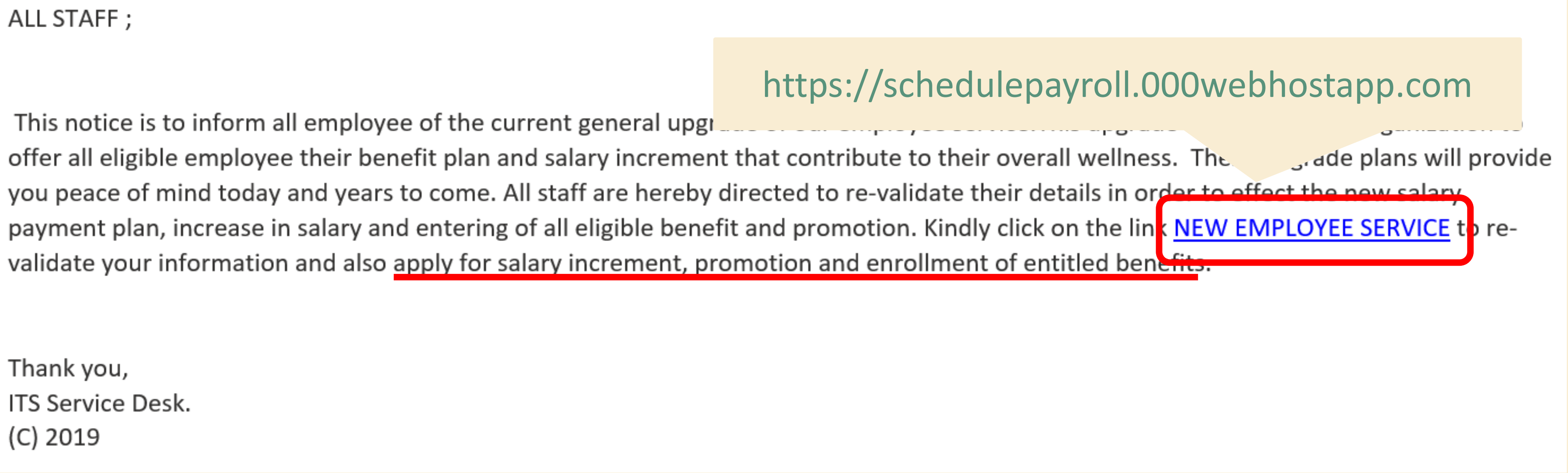
Average Percentage of Questions Answered Incorrectly

Figure 4 shows the average percentage of incorrect answers, by industry.

Percentage of wrong answers, by industry

What Can I Do To be Safe

Never click on a link – or an attachment - from an unsolicited email



ALL STAFF ;

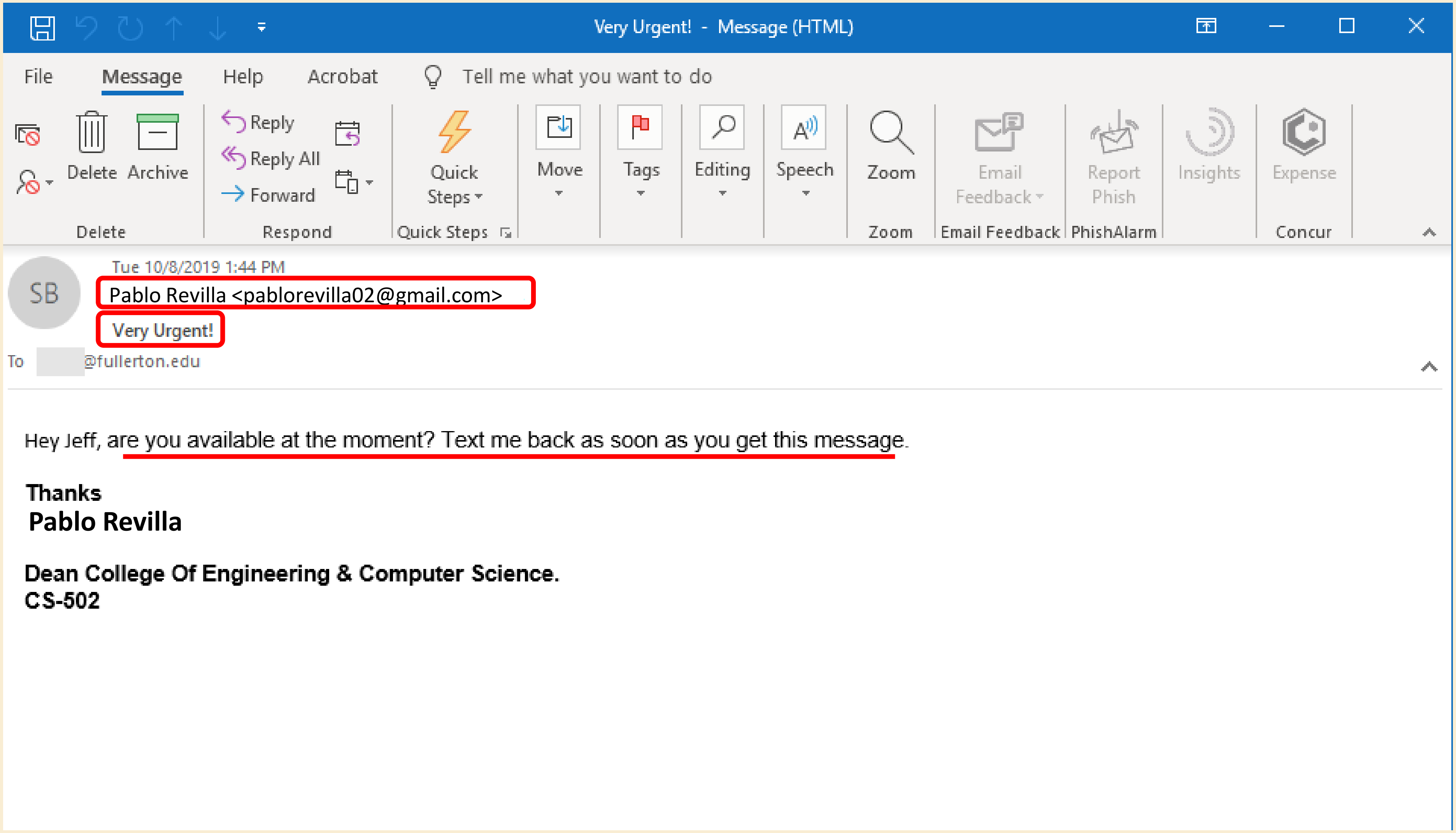
https://schedulepayroll.000webhostapp.com

This notice is to inform all employee of the current general upgr [illegible] offer all eligible employee their benefit plan and salary increment that contribute to their overall wellness. The [illegible] ade plans will provide you peace of mind today and years to come. All staff are hereby directed to re-validate their details in order to effect the new salary payment plan, increase in salary and entering of all eligible benefit and promotion. Kindly click on the link NEW EMPLOYEE SERVICE to re-validate your information and also apply for salary increment, promotion and enrollment of entitled benefits.

Thank you,
ITS Service Desk.
(C) 2019

What Can I Do To be Safe

Look for signs of Impersonation



Tue 10/8/2019 1:44 PM

Pablo Revilla <pablorevilla02@gmail.com>

Very Urgent!

To [redacted]@fullerton.edu

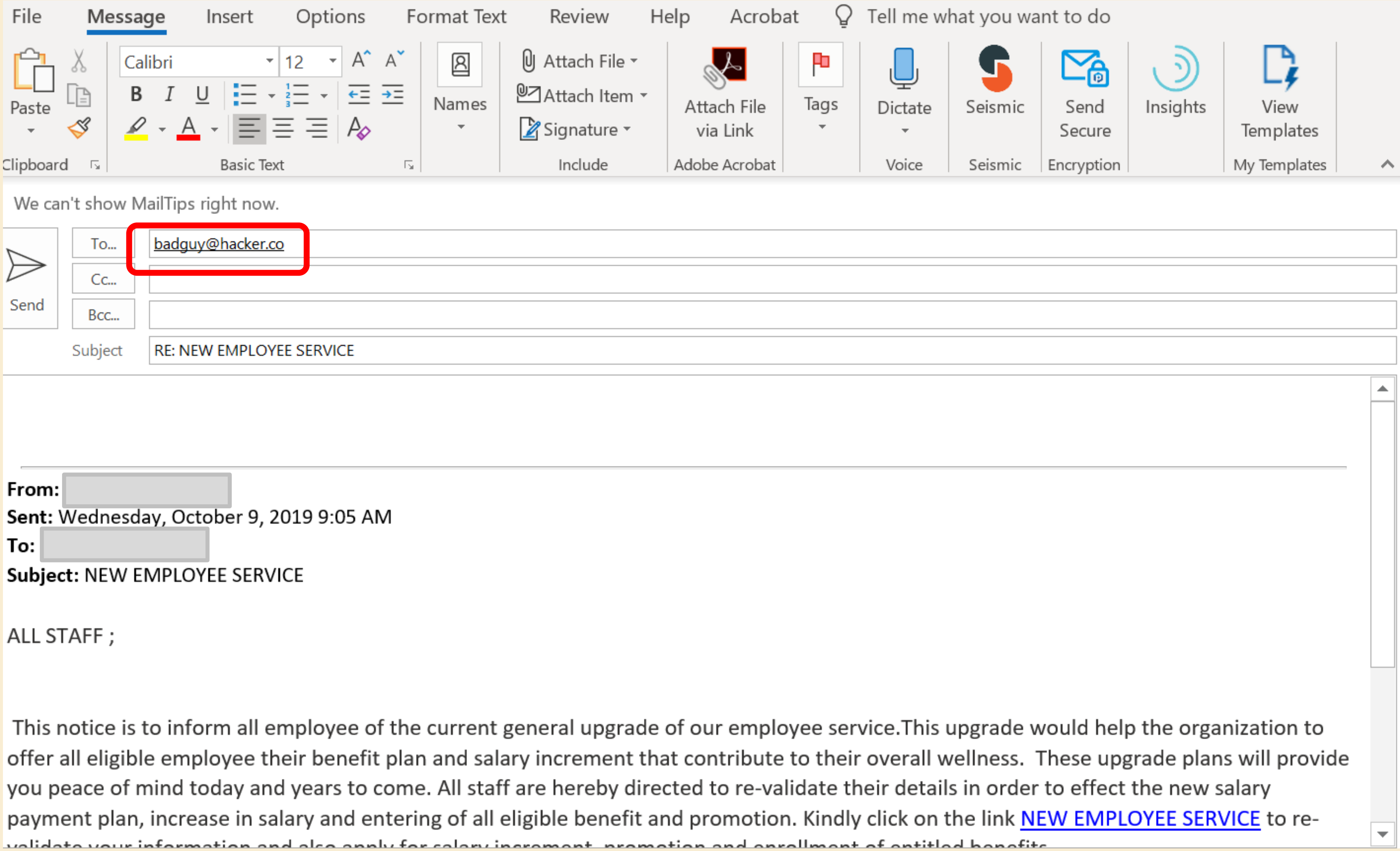
Hey Jeff, are you available at the moment? Text me back as soon as you get this message.

Thanks
Pablo Revilla

Dean College Of Engineering & Computer Science.
CS-502

What Can I Do To be Safe

Always look at the reply email address



We can't show MailTips right now.

To... badguy@hacker.co

Subject RE: NEW EMPLOYEE SERVICE

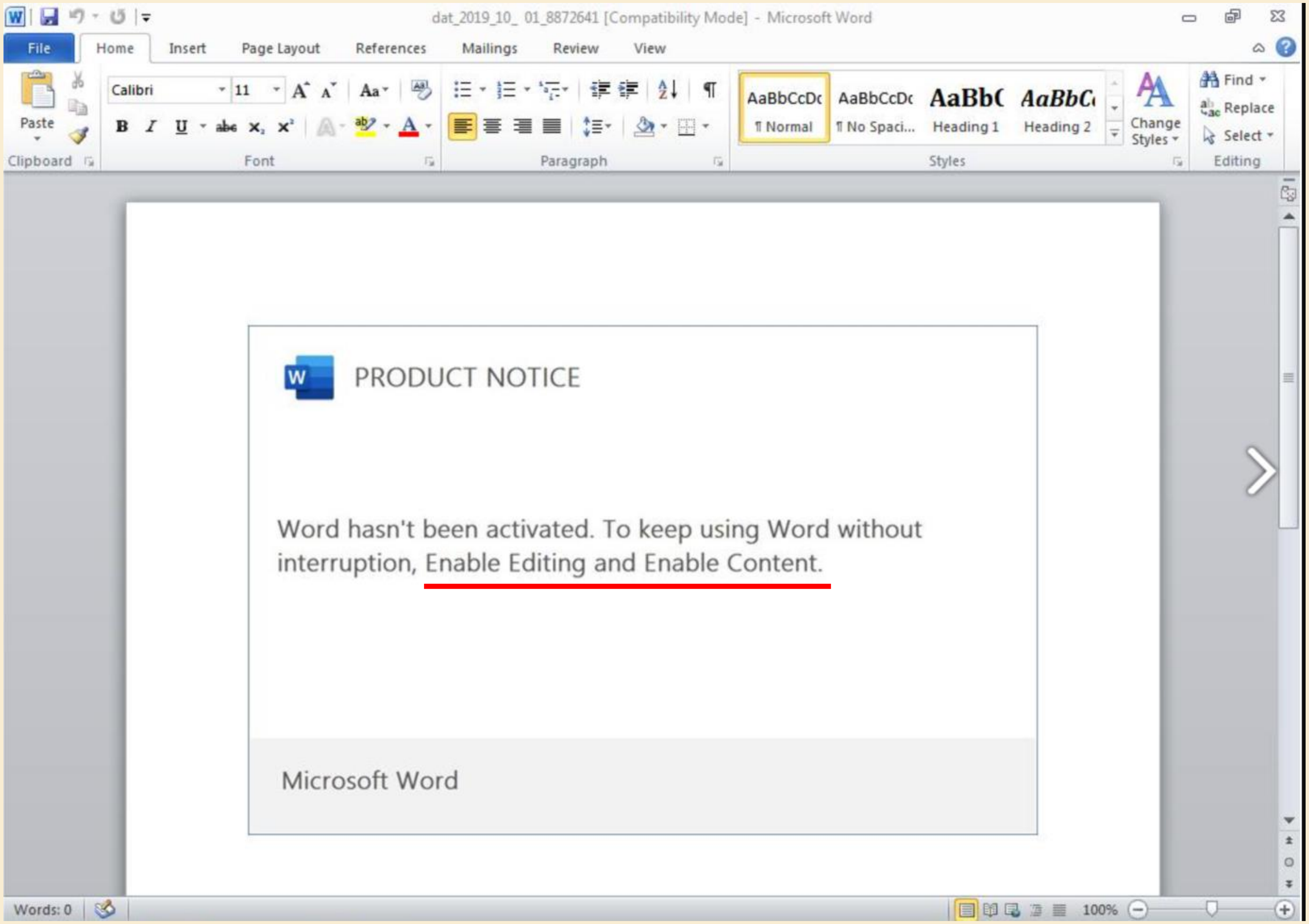
From: [redacted]
Sent: Wednesday, October 9, 2019 9:05 AM
To: [redacted]
Subject: NEW EMPLOYEE SERVICE

ALL STAFF ;

This notice is to inform all employee of the current general upgrade of our employee service.This upgrade would help the organization to offer all eligible employee their benefit plan and salary increment that contribute to their overall wellness. These upgrade plans will provide you peace of mind today and years to come. All staff are hereby directed to re-validate their details in order to effect the new salary payment plan, increase in salary and entering of all eligible benefit and promotion. Kindly click on the link NEW EMPLOYEE SERVICE to re-validate your information and also apply for salary increment, promotion and enrollment of entitled benefits.

What Can I Do To be Safe

Look carefully at attachments



PRODUCT NOTICE

Word hasn't been activated. To keep using Word without interruption, Enable Editing and Enable Content.

Microsoft Word

BE SAFE OUT THERE

- Never click on a link – or an attachment - from an unsolicited email

- Look for signs of Impersonation

- Always look at the reply email address

- **Look carefully at attachments** before you enable content or edit content

EXTRA

- Make sure your system and AV are UpToDate.