GOOD SECURITY STARTS WITH YOU

— Five Human Tactics to Stop Email Attacks —

mimecast®

The Human Target:
A CAUTIONARY TALE

Meet Jane. She is the financial controller at a medium-sized technology company and deals with confidential financial, employee and customer information every day. She is also authorized to approve financial transactions on behalf of Joe, the company CFO. When Jane received an email from Joe asking her to make a wire transfer to pay a contractor who was working on an office renovation, she didn't think twice: **The email came from a known source**, after all. So, she approved the transaction and carried on with her day.

This sounds like perfectly innocent and normal behavior, right? An employee receives an email from someone they know and responds accordingly. This is just part of a knowledge worker's day-to-day behavior.

Wrong.

"Joe the CFO" was actually a cyberattacker who targeted – and successfully duped – Jane. In about one minute, Jane became the victim of an email-based attack, costing the company $150,000.

Ouch!

This type of targeted attack is called whaling or Business Email Compromise, and it happens every day across organizations of all sizes and industries. And, whaling is just one attack method. There is an entire threat landscape evolving with every attack, fueled by methods like phishing, spear-phishing, domain spoofing, URL rewriting and you guessed it – whaling – to name just a few. Though these attack methods seem confusing and vary in technique, they do have one thing in common: email. Email is the number one entry point for cyberattackers to access data, credentials, money and even humans. In fact, **91 percent of hacking attacks begin with a phishing or spear-phishing email.**

Cyberattacks 101:

STOP. CHECK. CLICK.

It's ugly out there, people. No one is safe from being a target of a cyberattack. But, this doesn't mean we collectively surrender to cybercriminals. In fact, the opposite needs to happen. Every employee at every company, from the mom-and-pop shop to the midsize business to the enterprise giant, needs to mobilize and build a barrier against email attacks. We all need to do our individual part to build a solid human defense structure.

Before this can happen, you need to know what you're up against. Let's go back to Jane. If she had known about common types of attacks and what to look for, she may have thought twice before authorizing a fraudulent wire transfer.

Over the next three pages, you will learn the top-three attack methods that should keep you up at night – and yes, these attacks actually happened in real life.

The Attack Method

Phishing

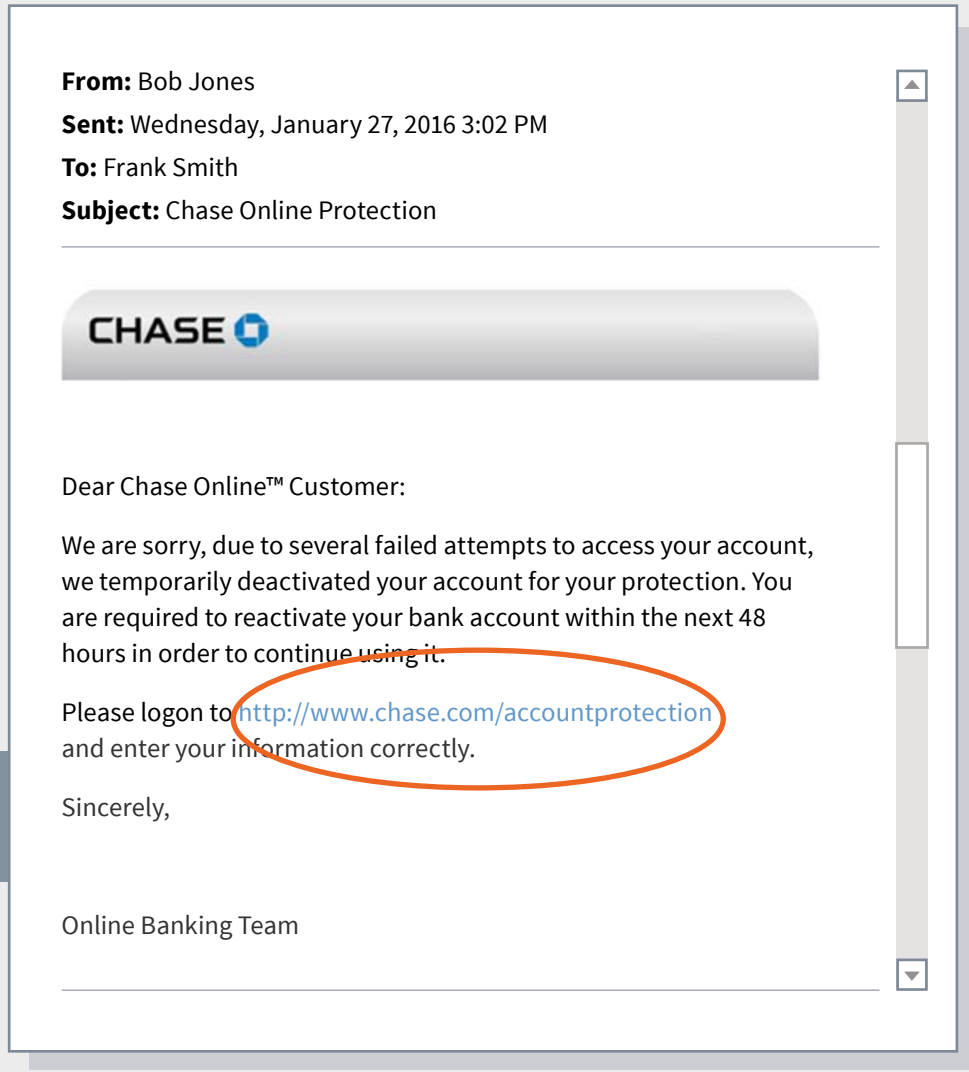
What Is It?

A form of fraud in which the attacker tries to obtain information, such as login credentials or account information, by masquerading as a reputable entity or person in email, IM or other communication channels.

The Dupe

A random, mass-mailing to thousands of possible Chase customers, prompting them to enter user credentials into a spoofed, malicious website.

Fake URL that goes to www.somewherebad.com



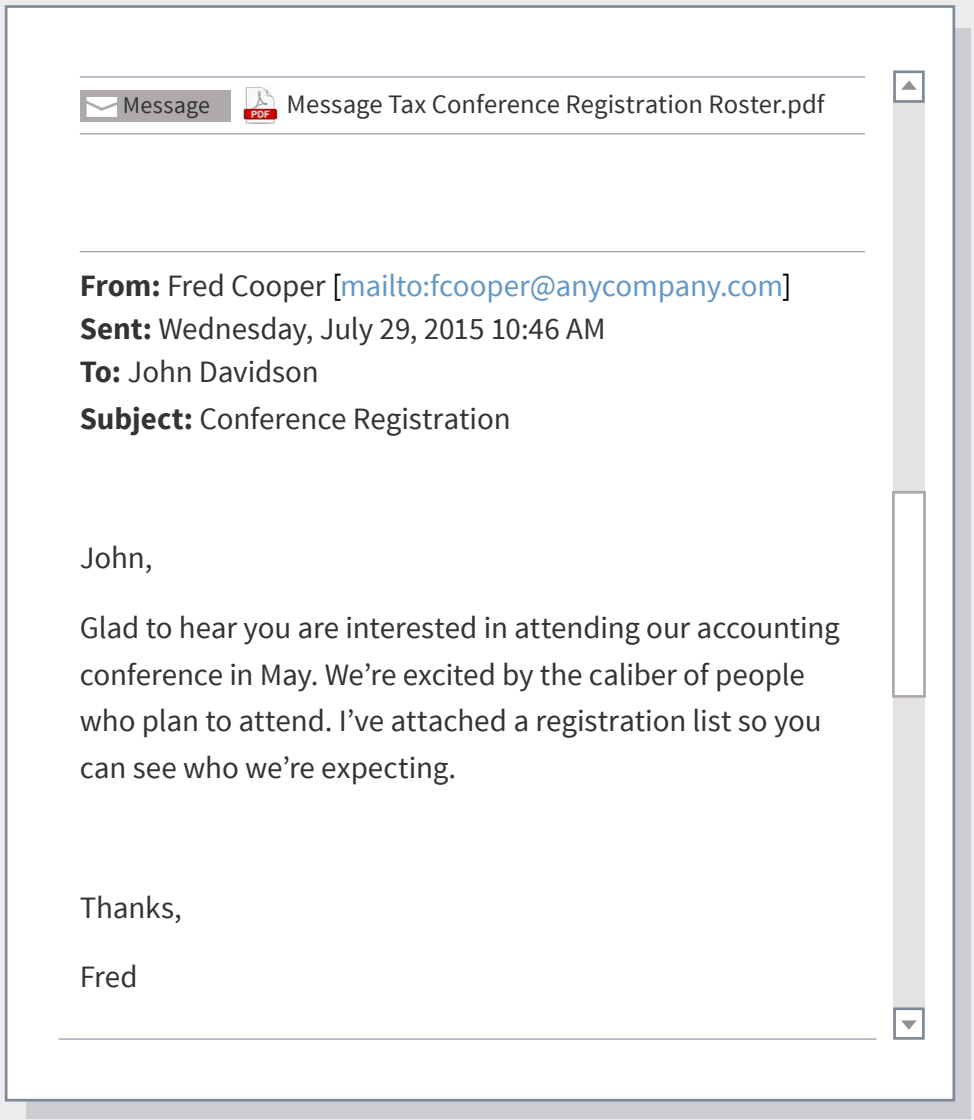
Spear-phishing

What Is It?

An email-spoofing fraud attempt targeting a specific organization, seeking unauthorized access to confidential data.

The Dupe

A cyberattacker does deep research on a particular company and target. Let's call the victim "John." The attacker knows that John is planning to attend an accounting conference in May just after tax season. Unwittingly, John has exchanged a couple of emails with the attacker, who is posing as an event organizer, after posting on LinkedIn that he plans to attend. Once the attacker sends the registration list in an attachment that's loaded with malware, it's just a matter of time before John opens it and becomes infected.



The Attack Method

Whaling, Business Email Compromise or CEO Fraud

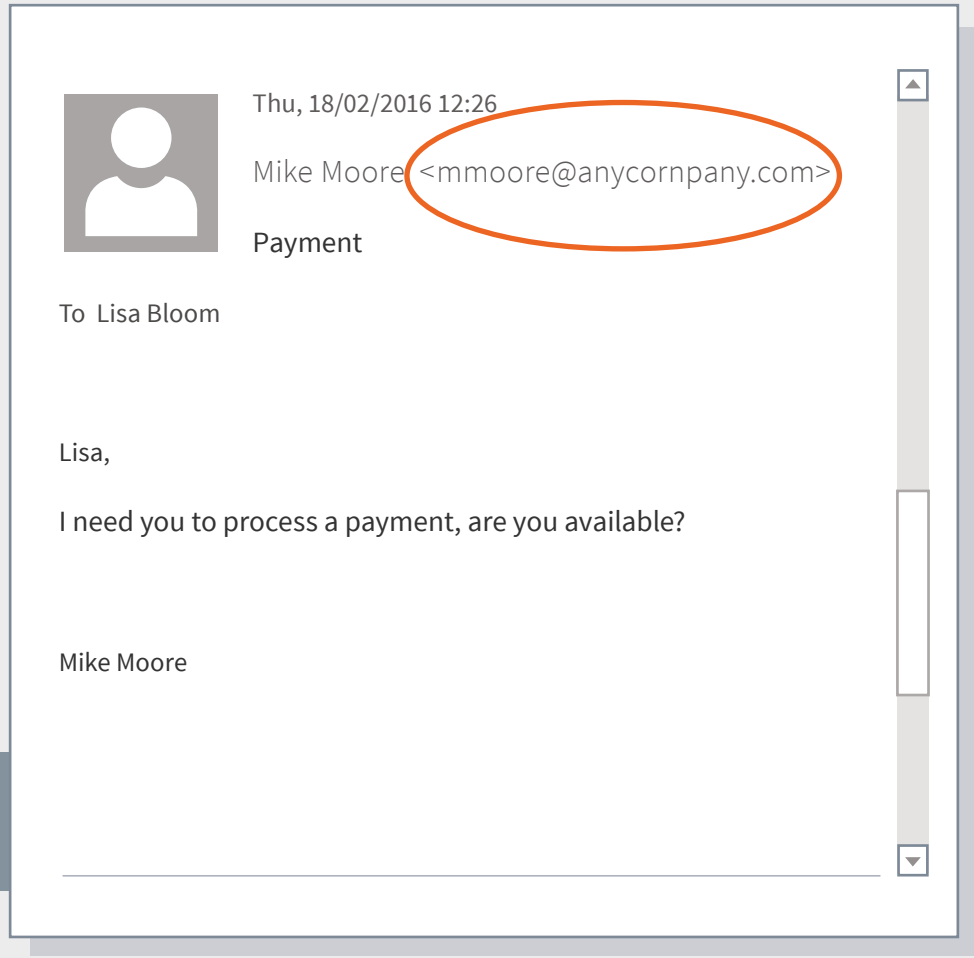
What Is It?

A sophisticated scam targeting organizations that regularly perform wire transfer payments and that hold important personal information on employees and customers. In short, all businesses!

The Dupe

The cyberattacker targets the financial controller at a company, impersonating the CFO. The email contains explicit instructions and instills a sense of urgency to add pressure to the decision-making process.

Fraudulent email address: Says “cornpany,” not “company.”



FIVE SECURITY TIPS TO LIVE BY

Defending an organization against cyberattacks is not just the responsibility of the IT team – it's the responsibility of every employee. Now that you know the three most common types of attacks, don't turn a blind eye. It's time to take action and this will take vigilance, awareness and a basic change in behavior.

Here are **five tips** to help you practice good security every day:

TIP 1

Pay attention! It's really that simple. It doesn't take a technical mastermind to carryout a hack – a cyberattacker just needs to access basic data, usually available to the public online. Next time you get an email from so-and-so at whatever bank requesting an employee's W-2 form, STOP. DON'T ACT. Forward the email to your direct manager or someone on your IT team. Think the email could be legit? Verify your hunch: Look at the domain name, website address and the sender's name to make sure there are no typos or intentional misspellings.

TIP 2

Remember the adage: "If it seems suspicious, it probably is."

If you receive an email that contains tracking information from a postal service, but you aren't expecting a shipment, STOP. Don't click the tracking URL because it's probably a malicious link disguised as something familiar. The same goes for emails containing attachments – these could contain malicious code.

TIP 3

Everyone's a target – but some have a public bullseye.

If you work in human resources, sales or communications, for example, it's likely your name and contact information are listed on the company's website. If this is the case, you need to be extra vigilant when it comes to practicing good security. Cyberattackers will view you as an easy stepping-stone to gain access to senior executives or company information. Be on the lookout for fraudulent emails, always.

TIP 4

Think before you share. Here's a wakeup call for you: Targeted attacks are not random. They are well-researched and usually architected using information you share online. Personal details like where you work, job title and whom you're friends with are plastered all over social media sites like LinkedIn and Facebook. Hackers research these sites to gather intel on unsuspecting victims – this is called Social Engineering.

Take Jane, for example. An attacker was able to see where she worked, her job function and connections. Voilà! A victim was born.

Cyberattackers will troll for the smallest detail on social media sites. Are you about to attend a company event? Share posts after the fact. Why? Think about it. Would you tell a burglar you're away and your house is empty? Also, if you receive a phishing email while distracted at an event or in a large crowd, you may not notice it's a scam. Cyberattackers know this.

TIP 5

Don't be a follower. After everything you just learned, this one should be a no-brainer. If you receive an email from a bank or financial institution requesting your credentials, don't click the link – it could be malicious. Even if the email is branded with what looks like legitimate logos and fonts, it could be a scam. Instead, type in the actual website address, verify the secure connection using "HTTPS" then provide your details in a legitimate, secure environment.

Good security practices don't have to be complicated. Remember: Before a cyberattacker can get their hands on data, employee information or money, they have to get through you. You have the power – and responsibility – to stop these insidious attacks.

mimecast®

To learn more, visit www.mimecast.com.

Mimecast (NASDAQ:MIME) makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.