# GOOD SECURITY STARTS WITH YOU

5 Tips to Fight Email-based Attacks

mimecast®

# THE HUMAN TARGET: A CAUTIONARY TALE

Meet Jane. Jane is the financial controller at a medium-sized technology company, so she 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 familiar contractor, she didn't think twice. **The email came from a known source, after all.** She approved the transaction and carried on with her day.


This sounds like perfectly innocent and normal behavior, right? 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 thousand.

**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, ransomware, domain spoofing and you guessed it – whaling – to name just a few.

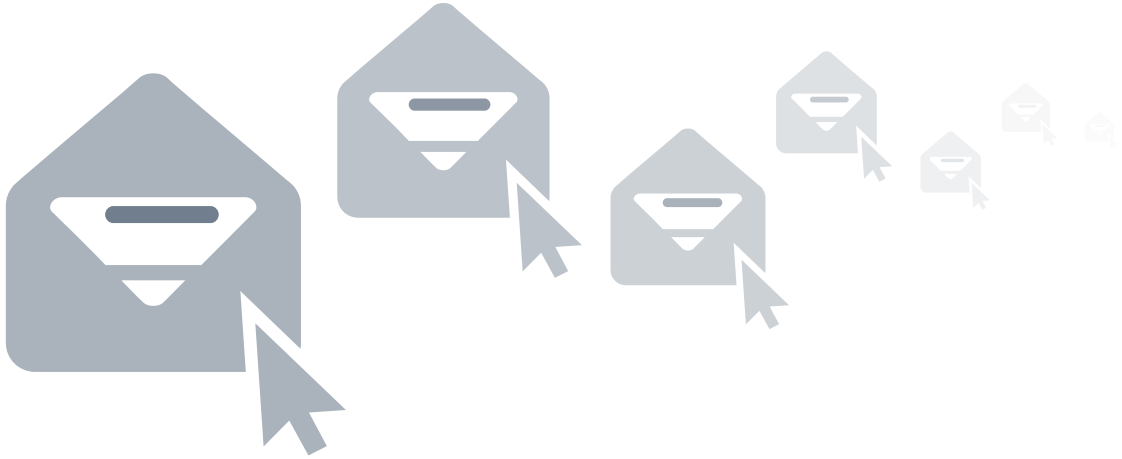
Though these attack methods vary in technique, they do have one thing in common: Email. Email is the number one entry point for cyberattackers to access data, credentials, money and even humans.

In fact, **99 percent** of ransomware attacks start with an email message, often enabled via phishing.

**99%**

**of ransomware attacks start with an email message.**

# STOP.
# CHECK.
# CLICK.



It's ugly out there, people. No one is safe from being a target of cyberattack. But, this doesn't mean we collectively surrender to the lords of cybercrime. In fact, the opposite needs to happen. Every employee at every company needs to strengthen their awareness on the different types of 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 cyberattacks, and what to look for, she may have thought twice before authorizing the fraudulent wire transfer.

**Turn the page to see 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 learn 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.

# THE ATTACK METHOD: RANSOMWARE


## What Is It?

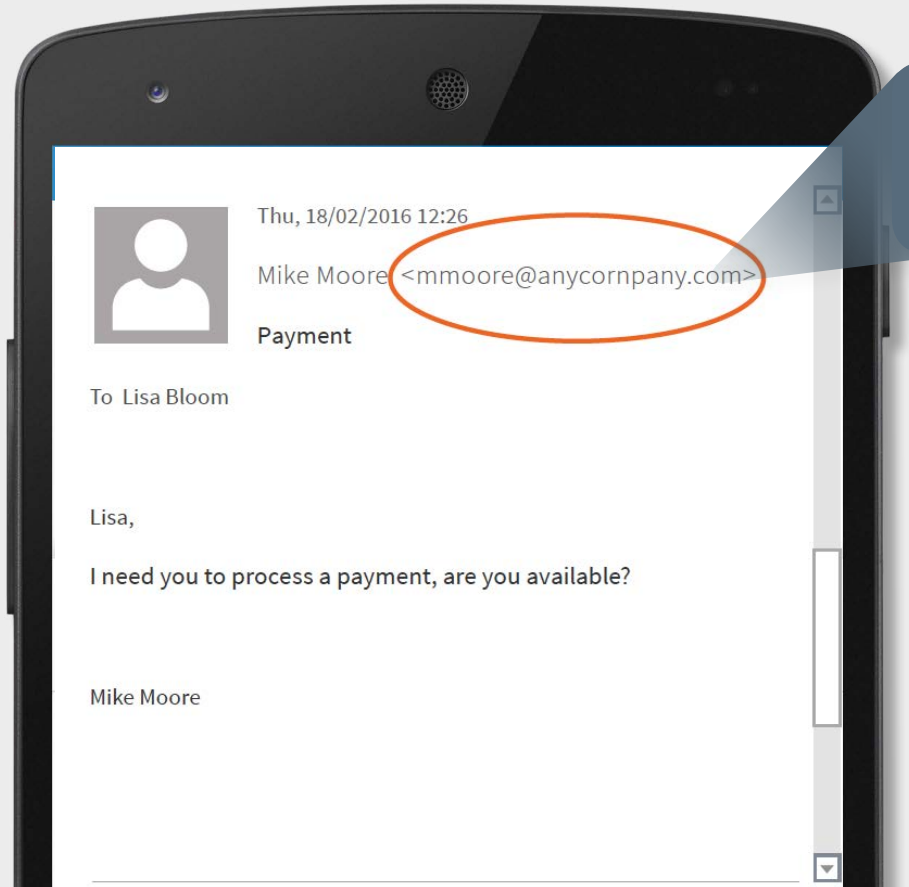

A file that looks seemingly innocent, but contains a malicious payload hidden in a standard document with active code. This code can then install key-logging software or run ransomware to lock-up your files or network drives.

## The Dupe:

The file containing the malware is disguised as tracking information for a scheduled delivery. It's designed to look like something familiar, and may even contain branding from a well-known delivery company. The user is encouraged to open the attachment in order to view the tracking information. This activates the active hidden code and locks-up the PC, files or network drives.

# THE ATTACK METHOD: WHALING

**What Is It?** A sophisticated scam targeting businesses that regularly perform wire transfer payments and that hold important personal information on employees and customers. In short, all businesses.




**Fraudulent email address:**
**Says "cornpany," not "company"**

## 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.

# DON'T BE THE ONE TO INFECT YOUR COMPANY

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

## *Here are five security tips to live by:*

1. **Pay attention!** It's really that simple. It doesn't take a technical mastermind to carry-out 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 W2 form, stop. 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.

2

**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 really a malicious link disguised as something familiar. The same goes for emails containing attachments – these could contain malicious code.

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 step-ping-stone to gain access to senior executives or company information. Be on the lookout for fraudulent emails, always.

4

**Think before you share.**
Here's a wakeup call for you: Cyberattacks are not random. They are well-researched and usually architected using information you share online. Personal details like where you work, job title, who you're friends with and what you're doing, when, 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.

**Remember Jane?** A cyberattacker was able to see where she worked, her job function and connections. Voila. A victim was born.


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®

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.

www.mimecast.com | 