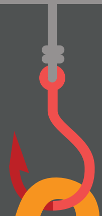
PROTECTING YOUR INBOX

9 easy ways to secure your email from the most common attacks

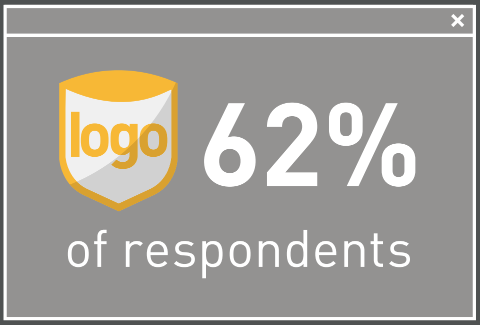
DON’T BECOME A STATISTIC!



94%

of people couldn’t tell the difference between a real email and a phishing email 100% of the time.

—McAfee: Phishing Deceives the Masses: Lessons Learned from a Global Assessment



62%

of respondents

in the global phishing study trusted an email that used a “spoofed” sender email address that appeared to be sent by UPS.

—McAfee: Phishing Deceives the Masses: Lessons Learned from a Global Assessment

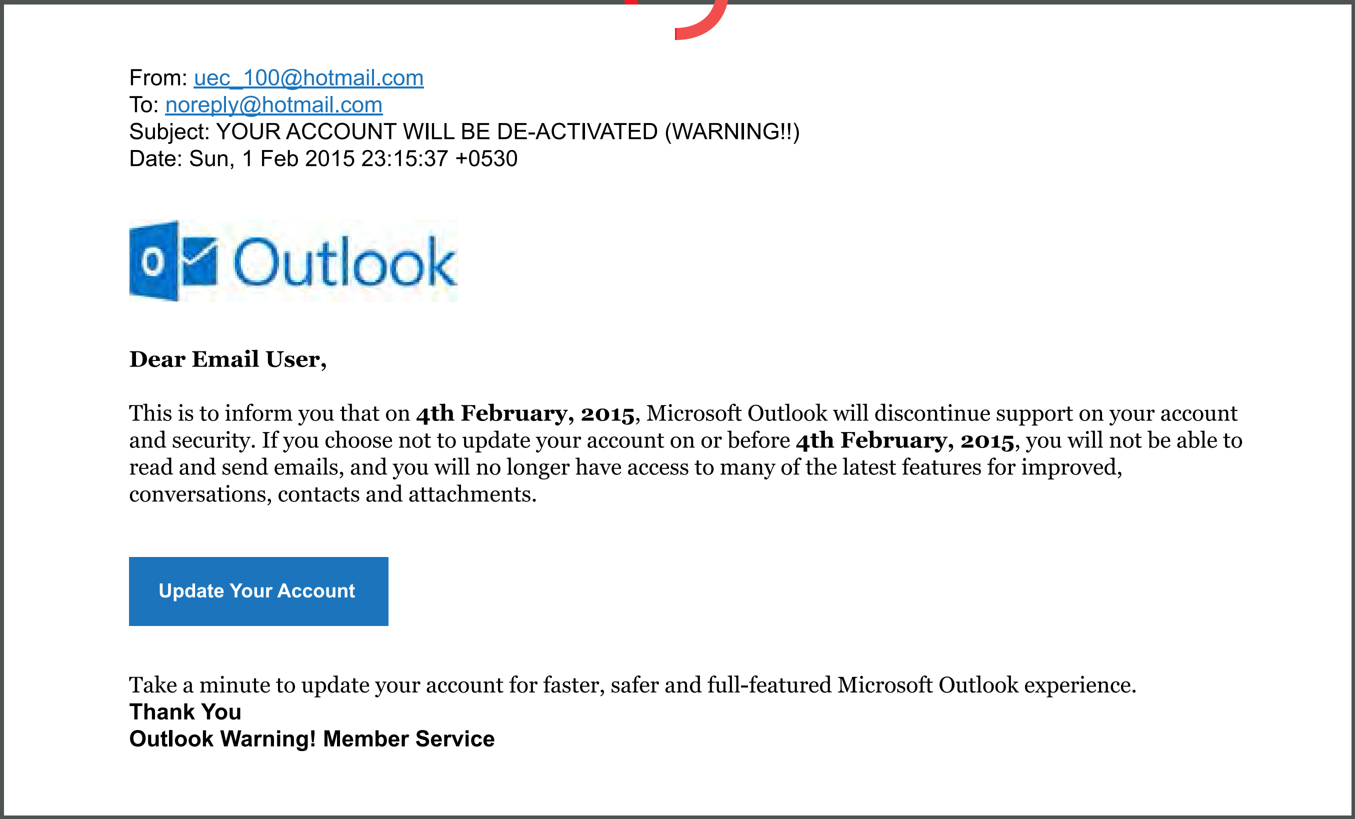
Nearly 1 in 5

users will click on a link within a phishing email.

– 2014 Verizon investigation report

“While people still look for identifiers such as sender’s name or address, subject line or content of the email, people tend to comply when a request comes from a figure of authority.”

– Hacking the Human Operating System: The role of social engineering within cybersecurity



From: uec_100@hotmail.com
To: noreply@hotmail.com
Subject: YOUR ACCOUNT WILL BE DE-ACTIVATED (WARNING!!)
Date: Sun, 1 Feb 2015 23:15:37 +0530

Dear Email User,

This is to inform you that on **4th February, 2015**, Microsoft Outlook will discontinue support on your account and security. If you choose not to update your account on or before **4th February, 2015**, you will not be able to read and send emails, and you will no longer have access to many of the latest features for improved, conversations, contacts and attachments.

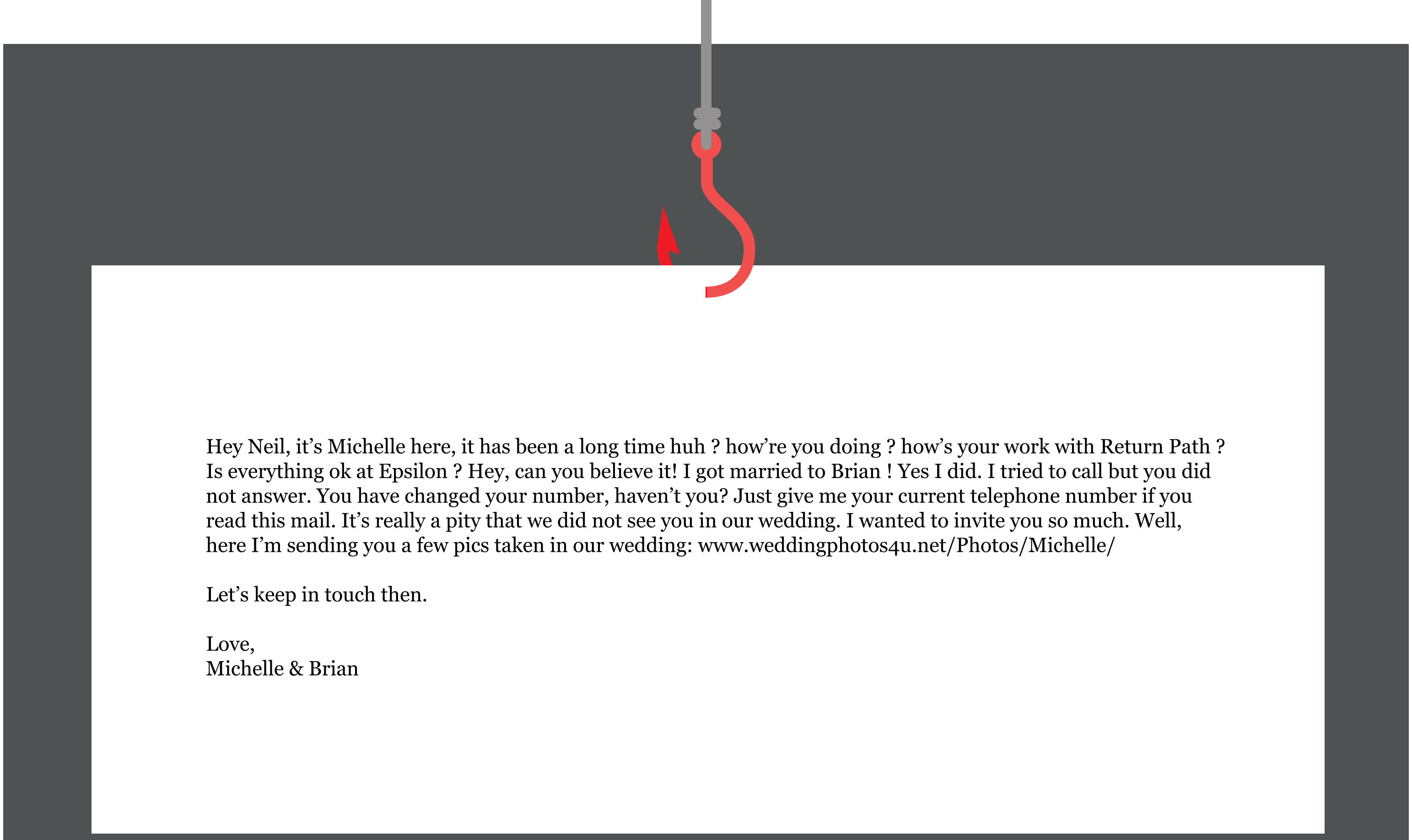
Take a minute to update your account for faster, safer and full-featured Microsoft Outlook experience.
Thank You
Outlook Warning! Member Service

Example of the Outlook.com phishing email.

Just this January, nearly 400 million Outlook.com users were sent an email like the one above.

If you had clicked to update your account, you would have been taken to a pretty convincing Outlook.com website and asked to enter your login credentials.

This is “phishing”, which presents a seemingly legitimate email that tries to get you to visit a malicious website or open a malware-laden attachment. The purpose is to capture your sensitive information: private documents, passwords, social security number, email contacts, credit card numbers, etc.



Hey Neil, it's Michelle here, it has been a long time huh ? how're you doing ? how's your work with Return Path ? Is everything ok at Epsilon ? Hey, can you believe it! I got married to Brian ! Yes I did. I tried to call but you did not answer. You have changed your number, haven't you? Just give me your current telephone number if you read this mail. It's really a pity that we did not see you in our wedding. I wanted to invite you so much. Well, here I'm sending you a few pics taken in our wedding: www.weddingphotos4u.net/Photos/Michelle/

Let's keep in touch then.

Love,
Michelle & Brian

Epsilon breach used four-month-old attack, iTnews.com.au

Phishing emails can be mass-mailers like the previous example, or they can be more personal. They can be highly targeted to you, which makes them even harder to spot. Take this email that was received by the employees in charge of email operations at Epsilon. It purported to be from a long lost friend. It seemed innocent – a friendly email announcing a recent wedding and including a link to view some photos.

Reports don't say how many Epsilon employees received the email or how many clicked on the link, but at least one person did. And it only takes one to infect an entire organization. The link in the email contained three pieces of malware that infected the user's computer, exposing the email marketing lists of many of their clients.

What happened to the staff at Epsilon was more targeted than regular phishing emails. The phishers chose specific people because of their role within the company. The emails those employees received mentioned their employer and played on the likelihood that people enjoy looking at photos.

HOW TO PROTECT YOURSELF

You can't rely on technology to fully protect you against these kinds of threats. You have an important role in email security.

Here are 9 easy ways to protect yourself and your company from common email threats. You can print out this handy sheet as a reminder. And if you have any questions, contact 3T Pro.

Email Security Checklist

BE AWARE OF EMAIL REQUESTS WITH HIGH URGENCY AND QUICK ACTION

If you are ever in doubt, double check the request with the sender either by phone or by composing a new email—never reply to the email itself.

NEVER GIVE PERSONAL OR FINANCIAL INFORMATION OVER EMAIL

Trusted parties will never ask you for personal information through email.
Try to make it a company policy not to collect employee information internally via attachments.

DON'T CLICK ON LINKS FROM MESSAGES THAT CONTAIN MISSPELLINGS

If an email from a well-known company is formatted badly, has obvious misspellings or is unrelated to the product or company, this is a red flag.

IF AN OFFER SEEMS TOO GOOD TO BE TRUE, IT PROBABLY IS

Big bonuses, large payments or gifts (ex. win a free iPad) for services are ways attackers try to get inside your head. If the promise is "too good to be true", do some research before taking action.

THINK ABOUT WHETHER YOU INITIATED THE ACTION

Phishers will try to spoof well-known companies, always be suspicious of unsolicited email, for ex. if you didn't prompt a password reset–don't click the link.

BE CAREFUL ABOUT WHAT YOU POST PUBLICLY TO SOCIAL NETWORKING SITES

If your social networking profile is public, avoid sharing birthdays, kids'names, or detailed business information because attackers will use it to get clues about what your passwords might be.

STAY EDUCATED ON TACTICS USED BY ATTACKERS

Currently, these attacks look like urgent emails coming from a boss or colleague, and attachments tend to look like a voicemail, fax or shipment tracking slip.

DON'T SEND OR STORE PASSWORDS IN EMAIL

Attackers that get access to your email account will search for anything of value and passwords are a high-value target.

ACT QUICKLY

If you accidentally click on a link or think that you have been phished, talk to your IT department, put a stop on a wire transfer or alert other people in the organization — immediately.

3T Pro Inc. - 100 N. Central Expy #1000 Richardson, TX 75080 - (972) 509-0585 - Support@3tpro.com