# PHISHING & EMAIL FRAUD PREVENTION

## 5 Fraud Tactics Your Employees Need To Be Aware Of

Retruster

# 1.

# AVOID THE URGE TO CLICK

We all have a side to us that's naturally curious, especially when it comes to finding out that a document is waiting for us, and that all we need to do is click to open it.

Is it important? Could it be interesting?

This is a classic scam used by fraudsters to get people to click on a compromised link to install malware, or even to get employees to to input their login information, which is then stolen – allowing hackers to get into your system, send emails as if they were that employee, and access sensitive information.

**"ALL YOU NEED TO DO IS CLICK A BUTTON"**


What makes matters even worse is that these types of scams often look like they come from legitimate, trusted sources, like Google Drive or Microsoft Sharepoint.

If you get a notification out of the blue that there is a document waiting for you, and all you need to do is click a button to open it, stop yourself right there and consider the consequences.

# 2.

# YOUR COMPUTER'S LIKELY NOT INFECTED

We've all seen the headlines about Ransomware spreading through computer systems and locking out users, until a Bitcoin ransom is paid. With names like Bad Rabbit and WannaCry (who names these things?!), they are enough to scare just about any internet user.

So of course one of the latest scams is faking a ransomware attack. An employee will get an email, announcing that the computer has been infected and that unless a ransom is paid by an imminent deadline, all data will be deleted.

Happily, the threat is an empty one (there has been no ransomware installed on the computer), but urgency is used by fraudsters to make people make mistakes. If you do get an email like this, report it immediately, do not take action or reply, and get that heart rate back to normal.

**For foolproof protection against these types of fraud, find out about Retruster**

# PROTECT YOUR BUSINESS BEFORE IT'S TOO LATE.

Learn More

# 3.

# OUT OF DATE DETAILS - DON'T BE FOOLED

## "JUST A FRIENDLY REMINDER TO UPDATE YOUR USERNAME AND PASSWORD, AS THEY ARE ABOUT TO EXPIRE"

"Just a friendly reminder to update your username and password, as they are about to expire".

Messages like these may seem friendly, but are actually a common way for hackers to gain access to your accounts.

And if, like many people, you use the same or similar passwords in different places, the results can be catastrophic.

These messages come in the form of very professional-looking emails, complete with official-sounding email addresses, so stay on the lookout. They are often sent from banks, or popular services like Apple and Netflix.

Not even government offices are immune, and a perennial favorite is to send official-looking documents from the tax man.

Who doesn't want to stay on the right side of the IRS?

# 4.

# ONE OF THE OLDEST IN THE BOOK


**RETRUSTER CAN AUTOMATICALLY PROTECT YOUR COMPANY AGAINST THESE TYPES OF FRAUD**

Almost like #3, but in reverse. This is a classic scam that has been around for as long as anyone can remember (although there's a twist).

In this instance, a regular supplier sends your team a message, informing you of updated banking details, or email addresses. What's different today, however, is that email addresses can be faked – so this looks like it's from someone you interact with regularly, but is really from a stranger.

Ideally, every message like this should be followed up with telephonically to confirm the change, however this is isn't always possible. Plus, if it came from the right email address, it must be legitimate, right?

Sadly, the answer is a resounding "No".

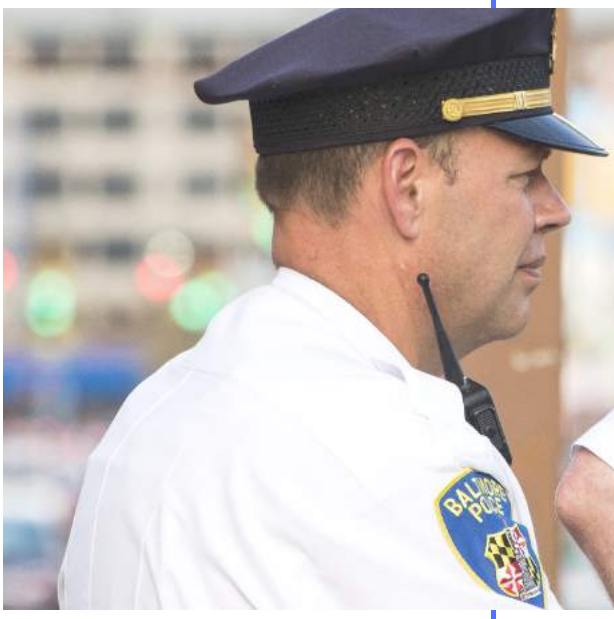
# PROTECT YOUR BUSINESS BEFORE IT'S TOO LATE.

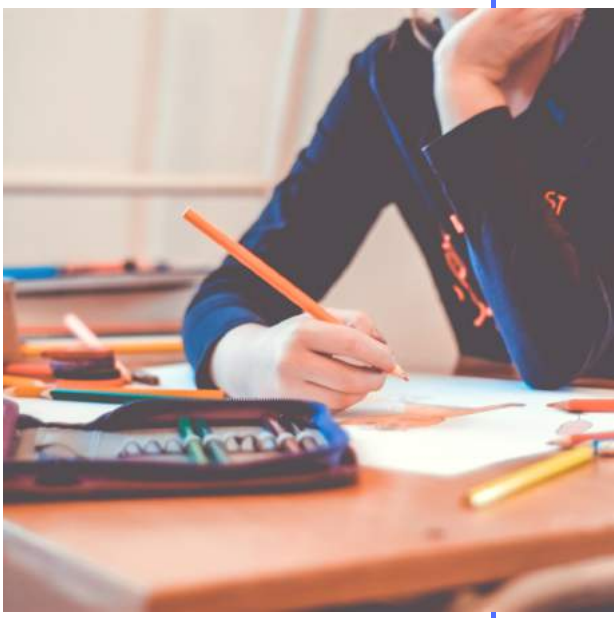
Learn More

# 5.

# TRUST ME, I'M A ____

## NO ONE CAN BE RELIED UPON, ESPECIALLY THOSE THAT WE WOULD NATURALLY TRUST MORE EASILY.





We are conditioned to trust certain people. Policemen, nurses, and college professors engender a certain amount of confidence.

Unfortunately, thieves and hackers are fully aware of this, and will be trying to dupe your employees with emails from “trusted” sources, whether it’s a local charity, a well-known personality, even members of the clergy.

Everything must be checked and checked again, and no one can be relied upon, especially those that we would naturally trust more easily.

# THE BEST WAY TO KEEP YOUR TEAM PROTECTED

**There are a few things that all of these latest scams have in common:**

- They affect us when we least expect it
- We can't detect there's a problem with a naked eye
- They take advantage of our sense of trust
- It's very difficult to check if they are valid or not

## RETRUSTER CHECKS EVERY INCOMING EMAIL AND LETS YOU AND YOUR TEAM KNOW IMMEDIATELY IF THEY ARE REAL OR FAKE

If anything suspicious is received by any of your team, Retruster flags it, quarantines it where necessary, and updates you.

You can see the overall picture from the Retruster dashboard, and for each problematic email, you'll see exactly why it's suspicious – empowering you and your employees.

Even when John in accounts has just pulled a pre-audit all-nighter, or your new intern with way too much energy is responding to every one of the three emails he gets every day -

**Retruster is there for your team to keep you protected against email fraud and "phishing" attacks, at all times.**

## FOR A DEMO: INFO@RETRUSTER.COM