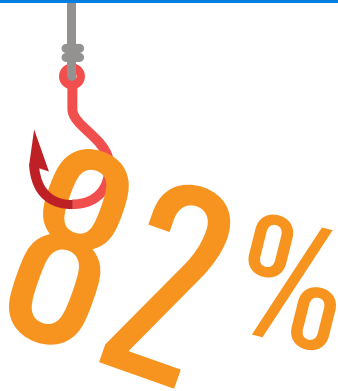


## 5 Easy Ways to Protect Yourself Against Phishing Attacks



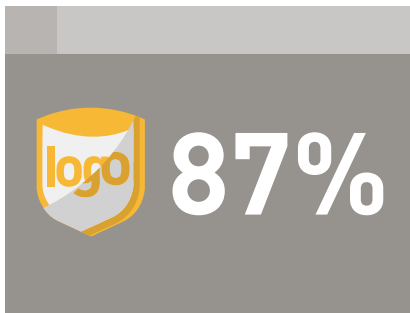
# DON'T BECOME A STATISTIC!



82%

of breaches involved the human element.

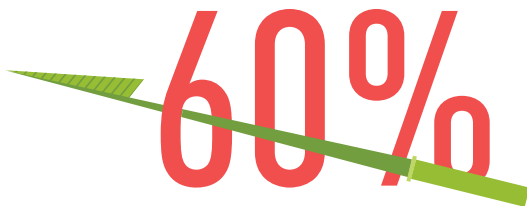
– 2022 Verizon Data Breach Investigation Report



87%

of credential phishing attacks looked like legitimate common business workflows in order to trick end users to engage with the message.

– Armorblox 2022 Email Security Threat Report



60%

of Social Engineering breaches involved Phishing

– 2022 Verizon Data Breach Investigation Report



“Phishing continues to walk hand-in-hand with use of stolen credentials in breaches as it has in the past.”

– 2021 Verizon Data Breach Investigation Report

# HOW TO PROTECT YOURSELF

You can't rely on technology to fully protect you against phishing threats. You have an important role to play in security.

Here are 5 easy ways to protect yourself and your company from common phishing attacks. You can print out this handy checklist as a reminder.



# PHISHING SECURITY CHECKLIST

1.

## BE AWARE OF REQUESTS WITH HIGH URGENCY REQUIRING QUICK ACTION

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

2.

## THINK ABOUT WHETHER YOU INITIATED THE ACTION

Phishers will try to spoof well-known companies or individuals. Always be suspicious of unsolicited messages, for example if you didn't prompt a password reset—don't click the link.

3.

## NEVER GIVE PERSONAL OR FINANCIAL INFORMATION OVER EMAIL OR TEXT

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

4.

## DON'T CLICK ON LINKS FROM MESSAGES THAT CONTAIN MISSPELLINGS

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

5.

## 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.



## 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.

Questions? Contact Us Today!

TSACHoice, Inc.

800.264.6878

customer@tsachoice.com  
www.tsachoice.com