



# Phishing Defense

## 👋 Hi there

Think you'd know if you were being 'phished'? 😬

Think again. From fake “unsubscribe” links to AI-generated scams that mimic real brands and websites, phishing attacks are getting smarter—and harder to detect.

Let's break down the tactics behind today's most convincing phishing threats, what to watch out for, and the habits that can keep you (and your company) safe. 🗉

## ✉️ What Is Phishing?



Phishing is a type of social engineering attack where criminals impersonate trusted sources—like your bank, employer, or even a friend. The goal is to trick you into:

- Clicking malicious links
- Downloading harmful files
- Sharing private information such as logins, credit cards, or personal IDs

Phishing attacks take place over SMS, email, phone calls, QR codes, or even work-related chat applications. Attackers thrive on creating urgency or fear to push quick, careless actions.

## 🤖 Smarter Scams with AI



Phishing is getting harder to spot. Scammers now use AI to:

- Write flawless, personalized messages
- Generate realistic fake websites
- Clone voices or videos to impersonate real people

These tactics make phishing attempts more convincing than ever, and as a result you have to more discerning than ever. Remember to always ask yourself: 'would my boss ask this?', 'would my insurance require this information over text?', and 'does this link look the official link online?' If you're hesitant about those questions—or any related questions—***don't reply.***

## 🌱 Test Your Skills!

### Instructions:

Test your phishing defense knowledge! Use the clues below to complete this cybersecurity crossword puzzle.



### Across

1. Scammers use this to write flawless, personalized phishing messages
4. This type of social engineering attack can be carried out over phone, email, text, and QR codes

### Down

2. Always do this before clicking a suspicious link
3. Never share this type of personal data over email or text

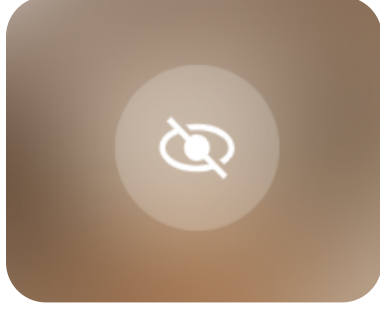
Answers: 1. AI, 2. Inspect, 3. Password, 4. Phishing

## 💡 How to Stay Safe



### 1. Pause and Inspect

Always check a sender's email address or a caller's number—make sure they are who they're claiming to be—and hover over any links you're set before clicking.



### 2. Don't Share Sensitive Info

Never send passwords to personal data over email, text, or chat service, even if the request seems urgent.



### 3. Report Suspicious Emails

If something feels off, report it to IT or your security team right away. It's always better to be safe than sorry.

👉 Phishing doesn't just target inboxes or phone numbers—it targets trust. The best defense is a workforce that slows down, inspects, and questions before they click. In a world of convincing fakes, vigilance is protection.

Your organization is partnering with Adaptive Security to offer you industry-leading security training.



902 Broadway, Floor 8  
New York, NY 10010