CYBER SECURITY INTERNSHIP AT

CODE ALPHA

PHISHING ATTACKS & CYBER AWARENESS

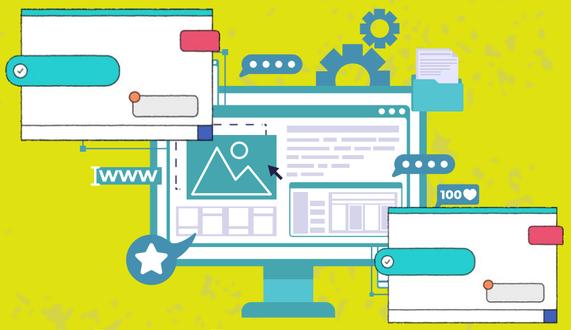
THINK BEFORE YOU CLICK. PROTECT THE HUMAN LAYER.

PRESENTED BY

DIXIT THUMMAR

STUD_ID : CA/DE1/2279

INTRODUCTION



WHY PHISHING AWARENESS MATTERS ?

Phishing is the #1 social-engineering threat — it targets humans, not systems.

Attackers exploit trust, curiosity, and urgency to trick users into mistakes.

KEY STATS :

$4.88M

avg. breach cost (IBM 2024)

68%

Breaches involve human error (Verizon DBIR 2024)

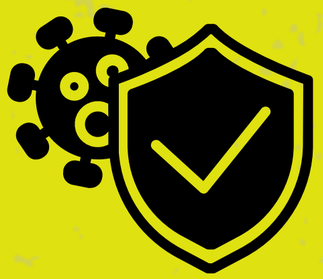
1M+

Phishing attacks in Q1 2025 (APWG)

GOAL OF THIS SESSION:

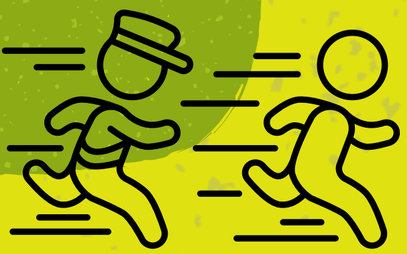
LEARN

IDENTIFY



PREVENT

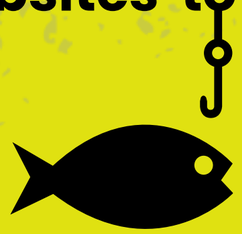
RESPOND



WHAT IS PHISHING?

DEFINITION:

- Phishing is when someone tricks you with fake messages or websites to steal your personal information or money.



CHANNELS:

- Email, SMS, Social Media, Phone Calls
- Attackers use psychological triggers like trust and urgency to make you click.

PILLARS OF PHISHING:

- 🤝 TRUST – LOOKS LEGITIMATE
- ⏰ URGENCY – ACT NOW PRESSURE
- 🏢 FAMILIARITY – KNOWN BRAND IMITATION

WHY HACKERS USE PHISHING ?

IT'S CHEAP, FAST, AND WORKS.
Phishing is the easiest way to access secure systems — through people.

KEY DRIVERS:

LOW COST, HIGH ROI — KITS UNDER ₹900

SCALABLE — THOUSANDS OF TARGETS VIA AUTOMATION

FACT: 94% OF MALWARE IS DELIVERED VIA EMAIL ATTACHMENTS.

HOW PHISHING WORKS ?(KILL CHAIN)

1.RECON (RESEARCH):

- Attacker collects basic information about the target from social media, company websites, etc.

1. LURE (TRAP):

- They send a fake email, message, or link to trick the person.

1. DECEIVE (TRICK THE USER):

- The victim is guided to a fake website or harmful link that looks real.

4.CAPTURE (STEAL INFO):

- The attacker steals passwords, OTPs, or installs malware.

5. EXPLOIT (USE THE STOLEN DATA):

- They take money, hack accounts, or sell the stolen data.

NOTE

MOST PEOPLE GET FOOLED IN THE DECEIVE STEP — THAT'S WHERE ATTACKERS MAKE THINGS LOOK REAL.

TYPES OF PHISHING

EMAIL

Fake emails trying to trick you.

SPEAR

A fake email made specially for you.

WHALING

Tricks made for big people like CEOs.

SMISHING

Fake or scam messages on SMS.

VISHING

Scam phone calls pretending to be real people (bank, police, etc.)

HTTPS TRAP

A fake website that looks safe because it shows a lock sign.

QUISHING

Scanning a bad QR code that sends you to a fake website.

PHARMING

Your browser is secretly sent to a fake website even if you type the right address.

ANGLER

Fake help accounts on social media trick you.

EMAIL PHISHING: RED FLAGS

LEGIT EMAIL SIGNS:

1. Correct Email Address -
   - support@amazon.com
   - help@bankofindia.co.in

2. Normal, Calm Message -
   - “Your order has been shipped.”
   - “Please review your monthly statement.”

3. Makes Sense to You -
   - You actually ordered something
   - You requested a password reset

FAKE EMAIL SIGNS:

1. WRONG OR WEIRD ADDRESS.
   - amaz0n-help@gmail.com
2. URGENT/SCARY TONE.
   - “Your account will close in 30 mins!”
3. ASKS FOR PRIVATE INFO.
   - “Send your OTP now.”
4. SPELLING MISTAKES.
   - “Your account is terminated.”
5. UNEXPECTED ATTACHMENT
   - Invoice.zip .
6. LINK GOES TO A FAKE SITE.
   - fake-login123.com

SMISHING & VISHING

SMISHING (SMS PHISHING) :

WHAT IT IS:
Scammers send text messages to trick you.

COMMON LIES:
Your bank account is blocked" or "You have a package waiting."

THE TRAP:
They want you to click a link to steal your passwords.

VISHING (VOICE PHISHING) :

WHAT IT IS:
Scammers call you on the phone.

WHO THEY PRETEND TO BE:
Bank staff, Tech Support, or Police.

THE TRAP:
They try to scare you into giving them money or details.

SIMPLE SAFETY RULES :

Don't Click : Ignore strange links in SMS.
Keep Secrets : Never tell anyone your OTP or Password.
Hang Up : If a call feels wrong, cut it. Call the bank yourself using the number on your card.

FAKE WEBSITES & HTTPS MYTHS

❌ FAKE WEBSITE	✅ REAL WEBSITE
Spelled wrong (e.g., amaz0n.com, go0gle.net).	Spelled correctly (e.g., amazon.com).
Has a lock 🔒 but the website name is wrong. 	Has a lock 🔒 AND the website name matches exactly. 
Blurry images, bad grammar, or looks "messy."	Professional design, clear images, perfect grammar.
Creates Panic: "Login NOW or lose account!" 	Calm: Provides information without rushing you.
Hidden info: No address or phone number.	Transparent: Easy to find "Contact Us" details.

CASE STUDY: THE "SHARK TANK" SCAM

THE VICTIM :

Barbara Corcoran (Star of TV show Shark Tank).

THE SCAM :

Email Phishing using a fake name.

THE METHOD :

- The bookkeeper received an email asking to wire $388,000 for a "real estate renovation."
- The email looked like it came from Barbara's assistant.
- The Trick: The scammer changed one letter in the email address (Typo squatting).
  - Real: assistant@barbaracorcoran.com
  - Fake: assistant@barbaracorcorn.com (Missing the 'a' in Corcoran).

THE RESULT : The money was sent immediately. It was lost.

LESSON LEARNED :

- ✅ Check the Spelling: Always read email addresses letter-by-letter.
- ✅ Double-Check Payments: If someone asks for money via email, call them on the phone to confirm.

HOW PHISHING TRICKS YOU

THE PSYCHOLOGY :

Hackers play with your emotions, not your logic — they make you react fast without thinking.

COMMON TRICKS :

- 👨‍💼 Authority : Pretend to be your boss or IT team
- 😨 Fear : “Your account will be blocked!”
- ⏰ Urgency : “Act now or lose access!”

HOW TO OUTSMART THEM:

- Stop and read carefully
- Verify the sender through a different channel (phone/chat)
- Ask yourself → “Why do they want me to act so fast?”

WHY PHISHING IS DANGEROUS

PHISHING DAMAGES PEOPLE, COMPANIES, AND SOCIETY.

FOR YOU:

- 💸 MONEY LOSS
- 🔐 IDENTITY THEFT
- 😞 STRESS

FOR COMPANIES:

- 📉 AVERAGE LOSS
- 💸 $4.88 MILLION
- 🏢 REPUTATION HIT

WORLDWIDE:

OVER $16.6 BILLION LOST YEARLY TO CYBERCRIME

💡 **FACT :**

ATTACKS FOUND WITHIN 200 DAYS SAVE ABOUT $1.2 MILLION ON AVERAGE.

PHISHING FACTS & WARNING SIGNS

2025 QUICK STATS:

- 68 % of breaches = human error
- 64 % of companies hit by fake business emails (BEC)
- 94 % of malware sent by email
- 1 million + phishing attacks in Q1 2025

RED FLAGS TO SPOT:

- ✅ Too-good-to-be-true offers
- ⚠️ Urgent or threatening tone
- 🔍 Misspelled domains or fake links
- 🖱️ Hover links to see the real site

STAY SAFE
PERSONAL & WORKPLACE

PERSONAL PROTECTION:

- Use a Password Manager
- Turn on Two-Factor Authentication (MFA)
- Keep your apps and system updated
- Report suspicious emails to security team

FOR ORGANIZATIONS:

- Use Secure Email Gateway (SEG)
- Enable SPF, DKIM, DMARC for domain security
- Run simulated phishing tests for employees
- Add a “Report Phishing” button in mail apps

IQ QUIZ

Q1: YOU RECEIVE AN EMAIL FROM “MICROSOFT SUPPORT” SAYING “YOUR ACCOUNT HAS BEEN COMPROMISED. CLICK HERE TO SECURE IT.”

Ⓐ CLICK THE LINK TO CHANGE YOUR PASSWORD

Ⓑ CHECK THE SENDER’S EMAIL AND GO DIRECTLY TO MICROSOFT’S OFFICIAL SITE ✅

Q2: YOU GET AN SMS FROM YOUR “BANK” SAYING “YOUR DEBIT CARD WILL BE BLOCKED. UPDATE YOUR KYC NOW!”

Ⓐ TAP THE LINK IN THE MESSAGE

Ⓑ IGNORE THE LINK AND CALL YOUR BANK USING THE OFFICIAL NUMBER ✅

Q3: YOU SEE AN ONLINE AD SAYING “CONGRATULATIONS! YOU’VE WON AN IPHONE 15. CLAIM NOW!”

Ⓐ CLICK IT AND FILL IN YOUR DETAILS

Ⓑ AVOID IT — IT’S A CLASSIC PHISHING LURE ✅

Q4: YOUR “HR DEPARTMENT” EMAILS A NEW FORM ASKING YOU TO ENTER YOUR LOGIN DETAILS TO VIEW YOUR SALARY SLIP.

Ⓐ LOG IN USING THE LINK INSIDE THE EMAIL

Ⓑ VERIFY WITH HR DIRECTLY BEFORE CLICKING ANY LINKS ✅

Q5: YOU GET A CALL FROM SOMEONE CLAIMING TO BE FROM “YOUR BANK’S FRAUD TEAM,” ASKING FOR YOUR OTP.

Ⓐ SHARE THE OTP TO CONFIRM YOUR IDENTITY

Ⓑ NEVER SHARE OTPS — NO BANK EVER ASKS FOR THEM ✅

CONCLUSION & KEY TAKEAWAYS

IF YOU FALL FOR IT:

- Disconnect from the internet
- Change passwords (on a safe device)
- Inform IT or Security team
- Run antivirus scan

REMEMBER:

- Humans = weakest link and strongest defense
- Always verify before you click
- “Phishing is inevitable — damage is optional.”
- Stay alert and protect the human layer.

THANK YOU

"SECURITY IS NOT A PRODUCT, IT'S A PROCESS."

DIXIT THUMMAR
DIXITTHUMMAR5@GMAIL.COM
https://github.com/Dixithummar
www.linkedin.com/in/dixit-thummar-450784363