PHISHING AWARENESS TRAINING

Protect Yourself. Stay Informed. Stay Safe

PHISHING AWARENESS TRAINING

PHISHING

Phishing is a type of cyberattack where attackers impersonate trusted entities to trick individuals into revealing confidential information such as passwords, credit card numbers, or personal data.

It is often carried out through fake emails, websites, phone calls, or messages.

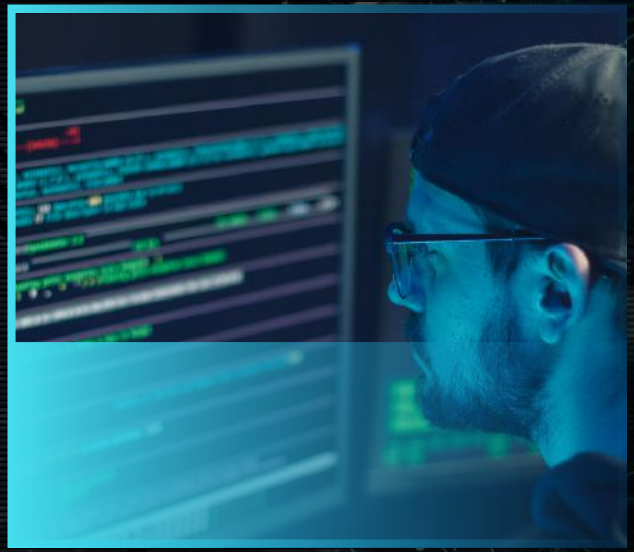
Phishing is one of the most common and dangerous forms of cybercrime, targeting individuals and organizations alike

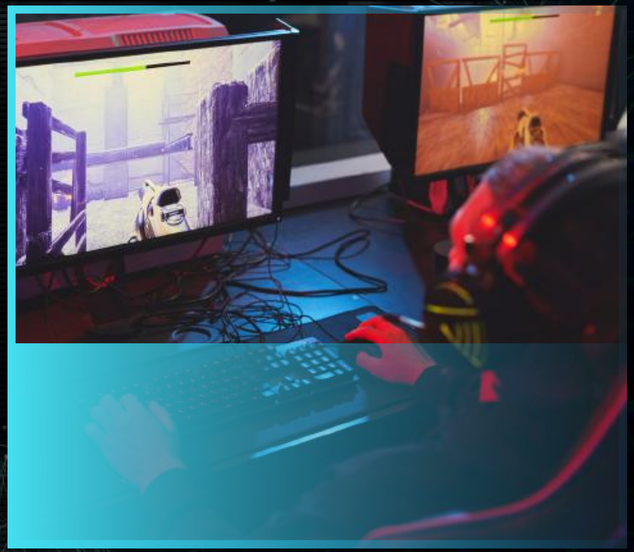
WHY PHISHING MATTERS

1. OVER 90% OF DATA BREACHES START WITH PHISHING. PHISHING CAN LEAD TO FINANCIAL LOSS, IDENTITY THEFT, AND SYSTEM COMPROMISE.

2. EVEN TECH-SAVVY USERS CAN BE TRICKED BY SOPHISTICATED SCAMS.

3. AWARENESS AND QUICK DETECTION ARE YOUR BEST DEFENSE.





COMMON TYPES OF PHISHING ATTACKS

- **Email Phishing**: The most common form — attackers send fake emails appearing to come from trusted companies (banks, services).
- **Spear Phishing**: Personalized attacks that target a specific person or organization, often using information from social media or company websites.
- **Smishing:** Phishing via SMS/text messages that include malicious links or requests.
- **Vishing:** Voice phishing through phone calls pretending to be tech support, banks, or government authorities.

REAL-WORLD EXAMPLE - WHAT CAN GO WRONG

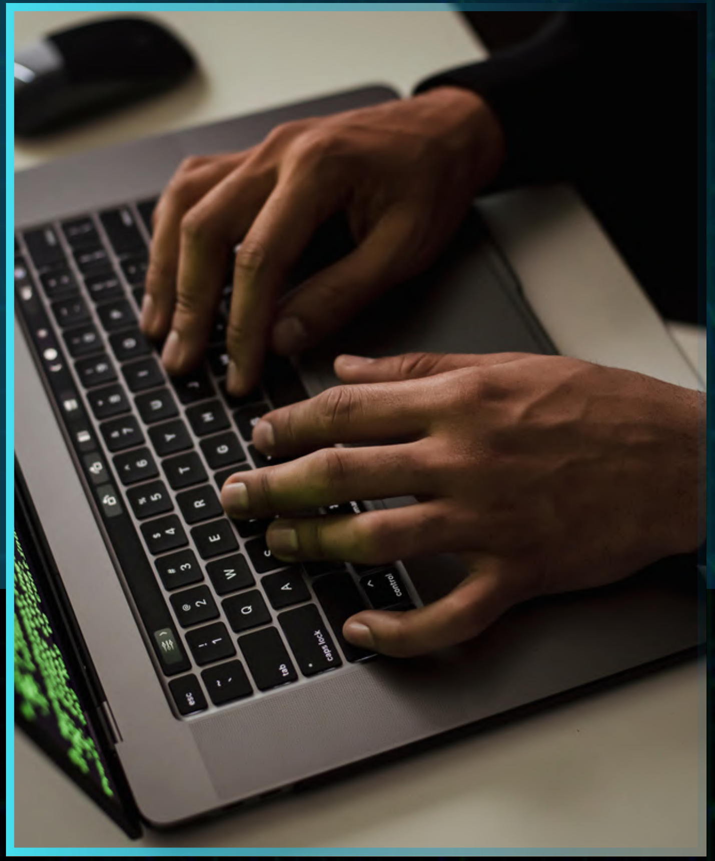
Case Study:

Between 2013 and 2015, a Lithuanian hacker tricked Google and Facebook into sending over $100 million by impersonating a hardware vendor via email.

- **Emails looked legitimate and followed invoicing procedures.**
- **Employees believed they were paying a real vendor.**

Lesson: Even top tech companies with expert teams can fall victim — vigilance is essential.

HOW TO SPOT PHISHING EMAILS



RED FLAGS IN A PHISHING EMAIL:

- Generic greetings like "Dear Customer"
- Urgent language: "Your account will be closed!"
- Misspellings and grammatical errors
- Suspicious sender addresses (e.g., support@micros0ft.com)
- Unexpected attachments or links
- Link preview (hovering shows a different URL)

HOW TO RECOGNIZE FAKE WEBSITES

- URLS THAT LOOK SIMILAR TO REAL ONES BUT HAVE EXTRA CHARACTERS OR MISSPELLINGS (E.G., WWW.FACEBOOOK.COM)
- LACK OF A SECURE CONNECTION (NO HTTPS)
- UNPROFESSIONAL OR BROKEN DESIGN ELEMENTS
- LOGIN PROMPTS THAT APPEAR ON PAGES YOU WOULDN'T EXPECT
- REQUESTS FOR SENSITIVE INFORMATION LIKE PASSWORDS OR PINS

TIP: BOOKMARK TRUSTED SITES. ALWAYS TYPE THE URL YOURSELF INSTEAD OF CLICKING LINKS IN EMAILS.

→

SOCIAL ENGINEERING TACTICS IN PHISHING

PHISHING ISN'T JUST TECHNICAL—IT RELIES ON HUMAN PSYCHOLOGY. ATTACKERS OFTEN USE:

- Curiosity: "See who viewed your profile"
- Fear: "Your bank account is locked!"
- Greed: "You've won a prize"

- Urgency: "Act now or lose access"
- Trust: Fake emails from your boss or IT department

BEST PRACTICES TO STAY SAFE

✅ Think before clicking — always verify the source
✅ Do not share sensitive info via email or message
✅ Check for secure (HTTPS) connections on websites
✅ Enable two-factor authentication (2FA)
✅ Use strong, unique passwords
✅ Keep your devices and software updated
✅ Report suspicious messages to your IT or security team

WHAT TO DO IF YOU SUSPECT PHISHING

1. Don't click any links or download attachments.
2. Take a screenshot of the suspicious message or website.
3. Report it to your IT department or security team.
4. Use the "Report Phishing" option in Gmail or Outlook.
5. If you entered credentials, change your passwords immediately.

REAL EMAILS VS PHISHING EMAILS

REAL EMAIL

- Sent from official domain
- No urgency or threat
- Personalized and relevant
- Secure links (with HTTPS)

PHISHING EMAIL

- Sent from lookalike or spoofed domain
- Creates urgency or fear
- Generic and often out of context
- Links go to shady or unknown domains

SUMMARY

- Phishing is common and growing more sophisticated.
- Learn to spot red flags in emails and websites.
- Trust your instincts — if something feels off, investigate.
- Stay informed, report suspicious activity, and encourage others to do the same.

THANK YOU
&
USEFUL RESOURCES

Thank you for participating!

Stay alert — cybersecurity starts with you.

Helpful links:

🔗 Phishing is common and growing more sophisticated.

- Learn to spot red flags in emails and websites.
- Trust your instincts — if something feels off, investigate.
- Stay informed, report suspicious activity, and encourage others to do the same.

🔗 Phishing is common and growing more sophisticated.

- Learn to spot red flags in emails and websites.
- Trust your instincts — if something feels off, investigate.
- Stay informed, report suspicious activity, and encourage others to do the same.

🔗 Phishing is common and growing more sophisticated.

- Learn to spot red flags in emails and websites.
- Trust your instincts — if something feels off, investigate.
- Stay informed, report suspicious activity, and encourage others to do the same.