Don't Get Hooked

A Guide to Spotting Phishing Attacks

We're All Targets

Hey there! Let's talk about something that happens to all of us - those sneaky attempts to trick us into giving away our personal information. Yep, I'm talking about phishing attacks.

Think about it - have you ever received an email that just seemed... off? Maybe it was supposedly from your bank, but something about it felt wrong? Or perhaps a text message with an urgent request to "verify your account"? If so, you've been targeted by phishing - and you're definitely not alone.

In 2024, over 90% of cyberattacks begin with a phishing attempt. The average person receives 16 malicious emails per month.

The truth is, phishing attacks aren't just annoying - they're dangerous. And they're becoming more sophisticated every day. But here's the good news: once you know what to look for, you can protect yourself and your information.

What is Phishing ?

At its core, phishing is simply digital deception. It's when someone pretends to be a trusted source to trick you into sharing sensitive information or downloading harmful software.

Types of Phishing Attacks You'll Encounter:

Type	Description	Common Targets
Email phishing	Mass emails impersonating legitimate organizations	Everyone with an email address
Spear phishing	Highly personalized attacks using your personal details	Employees, high-value individuals
Whaling	Targeting executives or high-profile individuals	CEOs, government officials
Smishing	Phishing via SMS text messages	Mobile phone users
Vishing	Voice phishing calls with scam scenarios	Everyone with a phone
Social media phishing	Fake profiles or messages on platforms like Facebook or LinkedIn	Social media users

Type	Description	Common Targets
Search engine phishing	Fake websites that appear in search results	Online shoppers, deal hunters
Clone phishing	Duplicates of previously sent legitimate emails with malicious links	Business professionals
Website spoofing	Fake websites that look eerily similar to legitimate ones	Online banking users, shoppers

Why It Works:

Here's the uncomfortable truth: phishing works because we're human. These attacks exploit natural human tendencies:

[Psychology of Phishing]

- **Trust**: We generally want to trust others, especially brands we recognize
- **Fear**: When threatened with account closure or security breaches, we react quickly and sometimes irrationally
- **Urgency**: When pressured to act fast, our critical thinking skills diminish
- **Curiosity**: Sometimes we just can't help but click on intriguing links or attachments
- **Desire for gain**: The promise of rewards, discounts, or free items can cloud our judgment
- **Authority**: We tend to comply with requests from perceived authority figures
- **Social proof**: If something seems normal or others appear to use it, we assume it's safe

Personal Reflection Moment: Think about a time when you almost fell for a scam. What emotion was the scammer trying to trigger in you? Fear? Curiosity? Excitement?

Red Flags: How to Spot a Phishing Attempt

Let's get practical. Here are the warning signs that should make your "phishing radar" go off:

In Emails:

🚩 **Mismatched or strange sender addresses**

- **Example:** support@g00gle.com instead of support@google.com
- **Look for:** Slight misspellings, additional characters, or unusual domains

🚩 **Grammar and spelling errors**

- Legitimate organizations have professional editors and proofreaders
- Multiple errors suggest the sender is either unprofessional or, more likely, a scammer

Generic greetings

- **Example:** "Dear Customer" or "Dear User" instead of your actual name
- Legitimate services that have your information will use your name

Urgent or threatening language

- **Examples:**
  - "Act now or your account will be permanently closed!"
  - "Immediate action required to prevent security breach"
  - "Limited time offer - respond within 24 hours"

Requests for sensitive information

- Legitimate companies rarely ask for passwords or full credit card details via email
- No legitimate organization needs your Social Security Number via email

Suspicious attachments

- Be extremely wary of .exe, .zip, .iso, or other executable files
- Document files (.doc, .pdf) can also contain malicious macros

Links that don't match where they claim to go

- **How to check:** Hover (don't click!) to see the actual destination in your email client
- Look for URLs that are similar to but not exactly the legitimate site (paypa1.com vs paypal.com)

On Websites:

Missing or incorrect HTTPS

- Secure sites should have HTTPS and a padlock icon in the address bar
- No padlock = no security = big red flag

🚩 **Slight URL variations**

- **Examples:**
  - netflix-account.com instead of netflix.com
  - annaz0n.com instead of amazon.com
  - paypa1.com instead of paypal.com

🚩 **Unprofessional design**

- Legitimate sites usually look polished and consistent
- Blurry logos, misaligned elements, and inconsistent formatting suggest a fake site

🚩 **Pop-up requests for personal information**

- Legitimate sites rarely use pop-ups to request login credentials
- Be especially wary if a pop-up appears immediately upon visiting a site

In Text Messages:

🚩 **Unknown senders with shortened links**

- Links like bit.ly or tinyurl can mask malicious destinations
- If you don't recognize the sender, don't click the link

🚩 **"Wrong number" texts that try to start conversations**

- **Example:** "Hey, is this John? I'm trying to reach you about the concert tickets."
- These often lead to romance scams or investment fraud

🚩 **Messages claiming to be delivery notifications**

- Especially suspicious when you're not expecting a package
- Legitimate delivery services typically don't send links in SMS

On Phone Calls:

🚩 **Requests for immediate action**

- Scammers don't want to give you time to think or verify
- "You must make a decision now" is almost always a scam

🚩 **Callers who won't let you call back**

- Legitimate organizations will provide a callback number
- Scammers often insist you stay on the line

🚩 **Requests for remote access to your devices**

- Very few legitimate situations require this
- Never give remote access to someone who called you

Real-Life Examples: Could You Spot These?

Example 1: The "Netflix" Email

![Netflix Phishing Example]

Subject: Your Netflix Payment Failed

Dear Customer,

We're having trouble with your current billing information. Please update your payment details within 24 hours or your account will be suspended.

[Update Payment Information Now]

Thank you for your cooperation, The Netflix Team

Red flags:

- Generic greeting ("Dear Customer" instead of your name)
- Urgent language creating artificial time pressure
- Suspicious link (hover to check where it really goes)
- No account specifics (which card failed, when the payment was attempted)

Example 2: The "IT Department" Message

![IT Phishing Example]

From: it-support@company-tech-helpdesk.com

Hello,

Due to a recent security incident, all employees must reset their passwords immediately by downloading and running the attached security update.

[security_update.exe]

IT Department

Red flags:

- Suspicious sender email (not matching your company's actual domain)
- Executable attachment (legitimate IT updates rarely come this way)
- Vague "security incident" with no specifics
- No signature from an actual IT team member

Example 3: The Banking Text

![Banking Phishing Example]

ALERT: Your [Bank Name] account has been temporarily suspended. Verify your identity at verify-bank-acct2.com to restore access.

Red flags:

- Suspicious URL (legitimate banks use their own domains)
- Urgent language
- Request for immediate action
- No personalization or account details

Example 4: The "CEO Email" (Business Email Compromise)

![CEO Phishing Example]

From: ceo.name@companyglobal-inc.org Subject: Urgent wire transfer needed

Hi [Employee Name],

I'm in a confidential meeting and need your help urgently. We need to pay a new vendor ASAP.

Please wire $24,850 to the following account: Bank: International Banking Corp Account: 5589327712 Name: Strategic Business Solutions LLC

Please keep this confidential and confirm when completed. I'll provide details later.

Thanks, Sent from my iPhone

Red flags:

- Suspicious domain (slightly different from company's real domain)
- Unusual request bypassing normal procedures
- Request for confidentiality to avoid verification
- Urgent timeline
- Sent "from iPhone" to explain formatting differences

Example 5: The Job Offer Scam

![Job Offer Phishing Example]

Subject: Your Resume Impressed Us - Remote Position Available

Dear Professional,

After reviewing your profile, we believe you would be an excellent fit for our remote Data Entry position. This role offers:

- $35/hour
- Flexible hours
- Work from anywhere
- No interview required

To begin, we require you to purchase home office equipment from our approved vendor. We will reimburse you with your first paycheck.

Click here to accept this offer: [START YOUR NEW CAREER]

Regards, HR Department Global Enterprises Inc.

Red flags:

- Too good to be true (high pay, no interview)
- Generic greeting
- Upfront payment required
- Vague company name
- No contact person named

Interactive Activity: Spot the Phish

Look at these examples and see if you can identify which are legitimate and which are phishing attempts:

Email 1:

Subject: Amazon Order Confirmation

Hello,

Thank you for your order #112-3456789-0123456. Your package will be delivered on May 13, 2025.

To track your package or make changes to your order, click here: [View Order]

Amazon Customer Service

Email 2:

Subject: Urgent: Your AppleID has been locked

Dear Valued Customer,

Your Apple account has been temporarily locked due to too many failed login attempts. To unlock your account, please confirm your information here:

[Unlock Account Now]

Apple Support Team

Email 3:

Subject: Your May Statement is Available

Hello Alex Johnson,

Your credit card statement ending in 3456 is now available online.

Statement Period: April 3 - May 3, 2025 Balance: $1,243.87 Minimum Payment: $35.00 Due Date: May 25, 2025

To view your complete statement, please log in to your account at our website.

Thank you, First National Bank Card Services

Answers:

1. Potentially legitimate (but always check the actual sender address and hover over links)
2. Phishing (urgent language, generic greeting, suspicious link)
3. Potentially legitimate (personalized, specific account details, directs you to website without providing direct link)

If You've Been Phished: What Now?

If you think you've fallen for a phishing attempt, don't panic. Take these steps immediately:

First 24 Hours: Emergency Response

1. **Change your passwords** for any potentially compromised accounts
    - Start with financial accounts and email
    - Use strong, unique passwords
2. **Contact the real organization** if you shared banking or credit card details
    - Use the phone number on the back of your card, not from the suspicious message
    - Request fraud alerts or credit freezes if necessary
3. **Run a security scan** on your device
    - Use reputable antivirus software
    - Scan for malware that might have been installed
4. **Enable two-factor authentication** on your accounts
    - This adds an extra layer of security even if passwords are compromised

Next Steps: Damage Control

5. **Monitor your accounts** for suspicious activity
    - Check bank and credit card statements carefully
    - Look for transactions you don't recognize, even small ones
6. **Report the phishing attempt**
    - To your IT department if it was work-related
    - To the spoofed organization (forward to their security team)
    - To authorities: Report phishing to the Anti-Phishing Working Group
    - In the US, report to the FTC at ReportFraud.ftc.gov
7. **Document everything**
    - Save copies of phishing messages (but don't keep clicking links!)
    - Note what information was compromised
    - Keep records of all your notifications and reports

Real Recovery Story:

"I clicked a link in what I thought was an email from my bank. I entered my login details before realizing something was off. Immediately, I:

1. Changed my bank password
2. Called my bank's fraud department
3. Enabled SMS alerts for all transactions
4. Set up credit monitoring

Three days later, I got an alert about an attempted large purchase that I didn't make. Because I had taken quick action, the bank had already flagged my account for suspicious activity and declined the transaction. Taking those immediate steps saved me from financial loss."

- Maria K., Phishing Survivor

Prevention: Your Anti-Phishing Toolkit

Here are practical habits to build your resistance to phishing:

Essential Daily Habits:

- **Verify directly**: Contact organizations through their official website or phone number (not the one in the suspicious message)
    - Type website addresses manually instead of clicking links
    - Use bookmarks for your important financial sites
- **Use multi-factor authentication (MFA)**: This adds an extra layer of security
    - Options include: SMS codes, authentication apps, security keys
    - Even if your password is compromised, MFA provides protection
- **Keep software updated**: This patches security vulnerabilities
    - Set devices to update automatically when possible
    - Don't postpone important security updates

Advanced Protection:

- **Use a password manager**: This helps you maintain unique passwords
    - Generates strong, unique passwords for each site
    - Often includes features to identify legitimate vs. fake websites
- **Consider email filtering services**: These can catch many phishing attempts
    - Many workplace emails have these built in

    - Consumer email services like Gmail and Outlook have some filtering
- **Check email headers**: These can reveal the true source of messages
    - Look for inconsistencies in the "From," "Reply-To," and originating server
- **Use security software**: These can help identify threats before you do
    - Look for solutions with phishing protection features
    - Keep definitions updated

Mental Habits to Develop:

- **Be skeptical**: If something seems too good to be true, it probably is
    - Unexpected winnings, inheritances, or job offers often signal scams
    - Legitimate organizations don't need urgent responses for routine matters
- **Take your time**: Legitimate organizations don't demand immediate action
    - Phishers create false urgency to bypass your critical thinking
    - When in doubt, step back and verify through official channels
- **Trust your instincts**: That feeling that "something's off" is often right
    - If an email feels suspicious, it probably is
    - When in doubt, verify through a separate channel

Protection Checklist:

- [ ] Use different passwords for important accounts
- [ ] Enable two-factor authentication where available
- [ ] Keep your devices and software updated
- [ ] Verify requests for information through official channels
- [ ] Be wary of unexpected attachments and links
- [ ] Check sender addresses carefully
- [ ] Use security software with phishing protection

Protecting Your Organization: Beyond Personal Defense

If you're responsible for protecting others in your organization:

Training and Awareness:

- Conduct regular phishing simulations to test awareness
- Share real examples of phishing attempts targeting your organization

- Recognize and reward vigilant behavior

Technical Controls:

- Implement email authentication protocols (SPF, DKIM, DMARC)
- Use email filtering and anti-phishing tools
- Consider advanced threat protection solutions

Response Planning:

- Create clear reporting procedures for suspicious emails
- Develop an incident response plan for successful phishing attacks
- Designate security champions across departments

Policy Development:

- Establish clear security policies around email handling
- Create guidelines for sensitive information requests
- Implement least-privilege access controls

Conclusion: Trust Your Instincts

At the end of the day, your gut feeling is often your best defense. If something feels off, it probably is. Don't click, don't download, don't share information - instead, verify through official channels.

Remember these key takeaways:

1. Legitimate organizations won't pressure you for immediate action
2. When in doubt, contact the organization directly using official channels
3. Be especially cautious with unexpected communications
4. Keep your security software and knowledge updated
5. Report suspicious activity to help protect others

It's better to be a little paranoid than to be phished. Stay alert, stay skeptical, and stay safe out there!

Quiz: Test Your Phishing Awareness

1. If an email has the correct company logo, it's probably legitimate.
    - True
    - False (✓ Correct: Logos are easy to copy)
2. Which of these is NOT a sign of a phishing attempt?
    - A message creating urgency
    - An email addressed to you by name with accurate account details (✓ Correct)
    - Requests for personal information
    - Links that don't match the hover text
3. What should you do if you're unsure about an email from your bank?
    - Click the link in the email to check if the website looks legitimate
    - Reply to the email asking for verification
    - Call your bank using the number from their official website or the back of your card (✓ Correct)
    - Delete the email and ignore it
4. A text message about a package delivery is always legitimate if you're expecting a delivery.
    - True
    - False (✓ Correct: Scammers often send fake delivery notifications)
5. What's the safest way to access your online accounts?
    - Click links from emails
    - Type the website address directly into your browser (✓ Correct)
    - Search for the website on Google
    - Use the same password for convenience
6. Which of these password practices provides the best security?
    - Using variations of the same password for different sites
    - Using a complex password and reusing it for important accounts
    - Using a password manager to generate and store unique passwords (✓ Correct)

- Changing your password every week but keeping it simple enough to remember

7. If you receive an urgent email from your CEO asking for an unusual wire transfer, you should:
    - Complete it immediately since it's from the CEO
    - Verify the request through a different communication channel (✓ Correct)
    - Reply to the email to confirm details
    - Delegate the task to someone else
8. Multi-factor authentication (MFA):
    - Is inconvenient and unnecessary
    - Only protects against some types of attacks
    - Provides significant protection even if your password is compromised (✓ Correct)
    - Is only needed for banking websites
9. Which type of phishing targets specific individuals using personal information?
    - Vishing
    - Smishing
    - Whaling
    - Spear phishing (✓ Correct)
10. After clicking a suspicious link, what should you do FIRST?
    - Turn off your computer
    - Change your passwords for important accounts (✓ Correct)
    - Ignore it and hope nothing happens
    - Format your hard drive

Additional Resources

- CISA Phishing Information
- FTC Advice on Phishing
- Anti-Phishing Working Group
- Have I Been Pwned - Check if your email has been compromised