



**proofpoint®**

## **Phishing 101**

Tips for spotting and avoiding email-based social engineering attacks

# What We'll Discuss

- What phishing is
  - Three primary phishing threats
  - Common hooks and social engineering techniques
  - Social engineering beyond the phish
- What phishing can do
  - Why cybercriminals choose phishing
  - Scope of phishing problem
  - Consequences of falling for phishing attacks
- How to identify and avoid phishing attacks



A photograph of a modern building with a large glass facade and a tiled roof, viewed from a low angle. The entire image is overlaid with a semi-transparent blue filter. The title text is centered on the left side of the image.

# Phishing and Social Engineering: The Basics

# What Is Phishing?

- Intentionally sounds like “fishing” because of how it works:
  - Emails that “fish for” information and access
  - Messages that “lure you in” and try to get you to “take the bait”
  - Once you’re “hooked”...you’re in trouble





# Three Primary Phishing Threats

- **Malicious links** – Take you to imposter websites that steal your info, infect your device with malware
- **Malicious attachments** – Compromise your computer
- **Requests for sensitive data** – Prompt you to fill in user IDs, passwords, financial information, etc., that is then stolen



# Social Engineering: The Art of Deception

- All phishing attacks use social engineering
- Social engineers use psychology to trick you
- Common social engineering techniques include:
  - Masquerading
  - Urgency
  - Making exciting



catch me



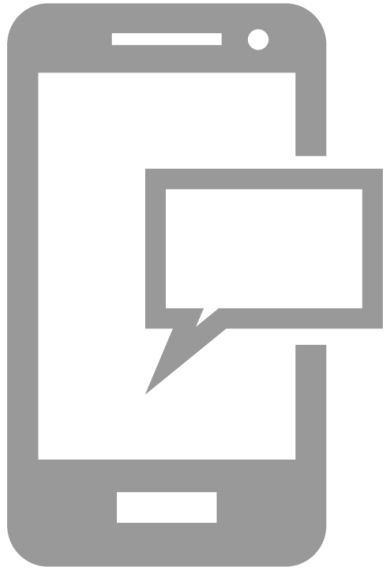
if you can

# Phishing Techniques: Not Just for Email

Social engineering tactics are used in multiple ways

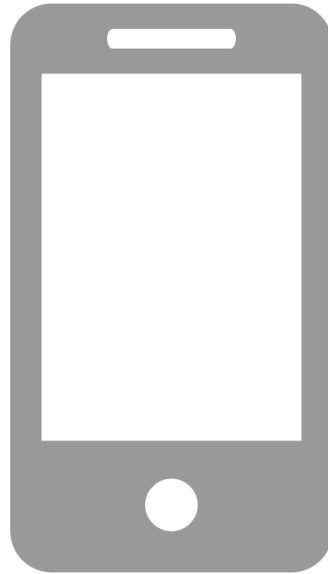
## SMS/text phishing

(also known as  
“smishing”)



## Voice phishing

(also known as  
“vishing”)



## Social media phishing

(via imposter accounts  
and malicious posts/IMs)





# How Phishing Is Impacting Individuals and Organizations



# Why Do Cybercriminals Love Phishing?

- Easy
- Cheap
- Effective
- Cybercriminals can get access to:
  - Money (via fraudulent wire transfers)
  - Financial, retail, social media, and email accounts
  - Contact names and customer lists
  - Important files and proprietary business information
  - Sensitive data (like tax information and medical records)
  - Servers, systems, and networks

# Why Do Cybercriminals Love Phishing?

- Phishing is easy for criminals because there is always something new to talk about
  - Data breaches can actually lead to new phishing attacks and more data breaches
  - Large-scale events and pop-culture references generate curiosity
- But don't forget about “tried and true” scams

# How Big Is the Problem?

- Nearly **900,000 unique phishing attacks** were reported between April 2018 and March 2019
  - Nearly **200,000 phishing websites** identified during the first quarter of 2019
- 
- More than **10 million** unsafe or unwanted emails are blocked **every minute**
  - Attackers send **6.2x more phishing emails** to corporate inboxes than personal inboxes
- 
- More than 30% of working-age adults **do not have a fundamental understanding** of phishing
  - **55% don't know what ransomware is**





# What Can Happen If You Fall for a Phish?

If you fall for a phishing attack, here are just **some** of the things that could happen:

## In Your Personal Life

- Money stolen from your bank account
- Fraudulent charges on credit cards
- Tax returns filed in your name
- Loans and mortgages opened in your name
- Lost access to photos, videos, files, etc.
- Fake social media posts made in your accounts

## At Work

- Loss of corporate funds
- Exposed personal information of customers and coworkers
- Outsiders access to confidential communications, files, and systems
- Files become locked and inaccessible
- Damaged employer's reputation

# Tips for Recognizing and Avoiding Phishing Attacks

# Attackers Use Many Tricks to Fool You

- Three main threats
  - Malicious links
  - Infected attachments
  - Phony requests for sensitive information
- No limit to types of messages
- Some attacks are personalized — may seem to be from someone you know
- Disguised phishing messages:
  - Requests from the IRS or other tax bodies
  - Software update notifications from trusted providers
  - Alerts from known banks, retailers, social media outlets, etc.
  - Notifications from internal departments like IT, HR, etc.



# You Are an Important Line of Defense

- Technical tools – like spam filters, anti-virus software, and firewalls – can't stop all attacks from reaching your inboxes
- Phishing emails are only successful if you take the bait
- Knowledge is power – it is the key to improving your cybersecurity hygiene

# Example of a Link-Based Phish

From: HelpDesk [mailto:xxxxx@connect.ust.hk]

Sent: Wednesday, April 12, 2017 2:23 PM

To: [redacted]

Subject: Validate Email Account

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

[Validate Email Account](#)

Sincerely

IT Help Desk

Office of Information Technology

The University

# Example of an Attachment-Based Phish

Subject: ID (k)dbm47-511-511-7465-7465

From: "Shipping Service" <user.vhj@detroit.com>

To:

Subject: ID (k)dbm47-511-511-7465-7465

Reply-To: "Shipping Service" <user.vhj@detroit.com>

Order: FD-24762590342635

**Dear Customer,**

Your parcel has arrived at the post office an November 19. Our postrider was unable to deliver the parcel to your.


To receive a parcel, please, go to the nearest our office and show this postal receipt.

Thank you.





# Example of a Request for Sensitive Data

 **GOV.UK**

**HM Revenue & Customs**

**Online Services - Refund form**

Due to a recalculation of your last fiscal activity you are eligible to receive a refund.

---

In order to receive the refund, submit a Tax refund request using the form below.  
Please enter your Personal information and a valid Credit / Debit Card where you want the refund to be made.

Full Name\*

Date of birth\*  
- Day -  - Month -  - Year -

Address\*

City\*

Postcode\*

Account number\*

Sort code\*

Number of reference: #5839158372

Refunds takes 30 business days to be processed.  
Do not submit invalid information.  
Submitting invalid information is prohibited by law.

# Tip #1: Read and Think Before You Click

## Thoroughly read emails. Watch for:

- Misspellings and poor grammar
- Messages that don't seem quite right
- Unsolicited emails

## Don't just react. Ask yourself:

- *Was I expecting this message?*
- *Does this email make sense?*
- *Am I being pushed to act quickly?*
- *Does this seem too good to be true?*
- *What if this is a phishing email?*

# Tip #2: Verify, Verify, Verify

## Be 100% confident you know the sender

- Logos are used illegally by scammers
- “Spoofing” can make From addresses, links, and caller ID look trustworthy
- In the case of a compromised email account, an attacker can send messages from someone else’s email account

## Don’t take messages at face value

- Hover over links to verify destination
- Confirm the email is legitimate
  - Instead of clicking a link, type a known URL into your browser
  - Instead of replying to the email or using a phone number from the message, use a verified, trusted contact channel

# Tip #3: Ask for Help

## At work

- Ask your manager or IT helpdesk for advice
- Report suspicious messages
- Responded to phishing message accidentally? Contact your IT team quickly!

## At home

- Trusted sites – IRS.gov, PayPal, Amazon, etc. – have advice about keeping your information secure
- Report spoofed phishing emails to the organizations they are mimicking
- Contact your bank, credit card company, tax organization, and/or local authorities in cases of lost/stolen funds, blackmail threats, or other crimes

# Stay Vigilant! Nobody Is Immune to Phishing.

- Make cybersecurity part of your daily routine
- Be particularly wary of emails that involve requests for:
  - Wire transfers
  - Tax and medical data
  - Financial account information
  - Password updates
  - File downloads
- Be on the alert for phishing techniques in text messages, on social media, and during unsolicited phone calls
- Report suspicious messages to your IT team

A man with glasses and a beard, wearing a dark suit over a light blue shirt, stands in an office or classroom setting. He is holding a tablet computer with both hands and looking off to the side. In the background, a chalkboard is visible with handwritten German text, including "nach am letzten", "Vorgang", and "Hauptbestand". The entire image has a blue color overlay.

# proofpoint®