Types of Phishing Attacks You Need to Know to Stay Safe
INTRODUCTION

Like Darwin's finches, phishing has evolved from a single technique into many highly specialized tactics, each adapted to specific types of targets and technologies. First described in 1987, phishing is now carried out via text, phone, advertising, and—of course—email.

Boiled down, all these tactics exist for the same purpose—to swipe confidential information from an unsuspecting target in order to extract something of value. But knowing about the hugely diverse set of today’s phishing tactics can help ordinary people, home and business internet users alike, to be more prepared for the inevitable instance when they become the target.

Here are 11 common phishing tactics you should know...
Most sources credit the first description of a phishing attack to a paper by the International HP Users Group, Interex in 1987.

STANDARD PHISHING
Casting a Wide Net

At its most basic, standard phishing is the attempt to steal confidential information by pretending to be an authorized person or organization. It is not a targeted attack and can be conducted *en mas*.

**An Example of Standard Phishing**

This tactic has, in the past, been more about quantity versus quality. The audience was broad and emails were riddled with noticeable errors. As phishing has developed, it’s become more sophisticated and harder to spot. Can you spot the red flags in the phishing email?

---

**The White House Instruction for Coronavirus**

`info@whitehousenovosinc.com`  
Jun 8, 2020, 1:09 PM (10 days ago)

Read the White House instruction for America about quarantine which will be prolonged till August 2020.

Protect yourself and your family from the pandemic by following official White House guidelines for slowing the spread of the virus.

*Steps to Stay Safe During the Pandemic*

Best,

White House Coronavirus Task Force
MALWARE PHISHING
Beware the Macros

How to Spot Malware Phishing

One hallmark of malware phishing is the attachment of a blank document requiring you to enable macros to view its contents, as in the common “package delivery failure” example below. This is a major red flag.

Received an unsolicited email from an unknown sender? Beware of downloading anything sent along with it. Many are malicious attachments known as ‘macros’.

Example of a malicious email attachment:

Package Delivery Failure: Schedule Your Redelivery

Dear customer,

We were unable to deliver your package because no one was present at your address.

Status: Failed
Date: 5 May 2020
Time: 10:15 am (EST)
Shipping Label: See attached

Please review the attached shipping information for item details, tracking numbers, and steps for requesting redelivery.

Note: We do not reply to this message. Customer service contact information is included in the attached document.

Copyright USPS. All rights reserved.
When the target is sizeable enough, spear phishing is sometimes called ‘whaling’.

A $24M Catch
SIM swapping is a type of spear phishing where attackers phish a target’s phone carrier, pretending to be the target to replace the SIM card with one of their own. One such case resulted in $24 million of lost cryptocurrency.

An Example of Spear Phishing
Below is a recreation of a real spear phishing attempt targeted at an MSP client.

Want to share and receive tips about ongoing scams with other cybersecurity-minded individuals? Join the Webroot Community.
SMS + PHISHING = SMISHING

Just Don’t Click

SMS-enabled phishing uses text messaging as a method for delivering malicious links, often in the form of short codes, to ensnare smartphone users in their scams.

Spotting a Smishing Attack
Be on the lookout. Smishing attacks often start something like:

- Your User ID and password are about to expire. Click here to reset your credentials before being locked out of your account.
- CBD has been proven to cause pain relief! Find out more.
- Changes were recently made to your Verizon account. Log in to configure your settings.
- You’ve won a $100 gift card!!! Click the link to redeem.

DID YOU KNOW?
SMS open rates hover around 98%. Compare that to around 20% for email, and it’s clear why cyber criminals like smishing.

Learn all you need to know about smishing and how to avoid it in this blog post.
SEARCH ENGINE PHISHING
Careful What You Choose

In this type of attack, cyber criminals wait for you to come to them. Search engine phishing injects fraudulent sites, often in the form of paid ads, into results for popular search terms.

Search engine phishing sites often promise amazing deals, career advancement opportunities, or low interest rates for loans. Remember, if it seems too good to be true, it probably is.

Detecting a Search Engine Phishing Scam

Often, the only difference between the scam result and the one you're looking for is a .com that should be a .org. Scrutinize the URL, meta title, and meta description before clicking. For an additional layer of security use a tool such as the Webroot Filtering Extension to flag potential threats, as in the image below.
VISHING
Keeping You On the Line

Vishing involves a fraudulent actor calling a victim pretending to be from a reputable organization and trying to extract personal information, such as banking or credit card information.

Most often, the “caller” on the other line obviously sounds like a robot, but as technology advances, this tactic has become more difficult to identify.

Riiiiing riiiiing riiiiing ... Hello, I'm with Windows Technical Support. I'm calling because your computer has been infected by a virus.

How to Avoid Vishing Scams

1. Be skeptical when answering calls from unknown numbers.
2. If they ask for personal information, don’t provide it over the phone.
3. Use a caller ID app, but don’t trust it completely.
4. Search for the caller’s phone number online to see if it’s a known scam.
5. If the call is about a product or service you use, go to the vendor’s website or call the vendor directly to confirm.

Being Vished?
Here’s What to Do.

Each tax season, vishing makes the IRS’s “Dirty Dozen” list of scams targeting Americans. It asks that these be reported to phishing@irs.gov.
DNS acts as the phonebook of the internet, taking a long string of numbers—the IP address—and translating it to the URLs we all know, like amazon.com. When cybercriminals interfere with this communication, it’s known as DNS poisoning.

**Operation Sea Turtle**

Given the level of technical sophistication it requires, DNS poisoning is often carried out by state-backed hackers. In one of the most famous examples, a group known by the code name “Sea Turtle” used the technique to spy on governmental intelligence agencies across the Middle East and North Africa. The attack was announced by the private intelligence group Cisco Talos in 2019.
Outlook, Gmail, and other email providers enable you to check the locations from which people have accessed your account. If you find your email has been compromised, follow these steps.

What Clone Phishing Looks Like

Below is an example of just how tricky clone phishing can be to spot. By exploiting social trust, the hacker increases the chances of spreading the infection.

![Image of email]

**Subject: RE: Sales Numbers (Adding Phil)**

Hi Team,

Resending to add Phil to the chain. Please remember to download and fill out the attached spreadsheet as soon as possible.

Kind Regards,

Ryan
MAN-IN-THE-MIDDLE
The Public WiFi Phisher

A man-in-the-middle attack involves an eavesdropper monitoring correspondence between two unsuspecting parties. When this is done to steal credentials or other sensitive information, it becomes a man-in-the-middle phishing attack. These attacks are often carried out by creating phony public WiFi networks at coffee shops, shopping malls, and other public locations. Once joined, the man in the middle can phish for info or push malware onto devices.

On most personal computers, especially those running on Windows operating systems, local file sharing is turned on by default. To prevent malware from being pushed to your device, toggle this setting to off when on unfamiliar networks.

How MIM Phishing Works
A victim trying to log into his bank account, for example, unknowingly sends his credentials to the attacker. The attacker then logs the victim in to the account so no suspicions arise.
BUSINESS EMAIL COMPROMISE (BEC):
Don’t Make the Payment

One of the most expensive threats facing businesses today is business email compromise. This involves a phony email usually claiming to be an urgent request for a payment or purchase from someone within or associated with a target’s company.

The Classic BEC Scheme

One of the most famous templates for achieving business email compromise is a frantic request by a supposed superior for gift cards. Often supported by publicly available information like a recently closed business deal, these common attacks ask for a rush delivery of gift cards from a large retailer be delivered to an address controlled by the malicious actor.

Look familiar?
“As a thank you to X client, I need you to mail $3,000 in Target gift cards to their head of procurement ASAP!”

Of the $3.5 billion the FBI estimates businesses lost to cybercrime in 2019, nearly half ($1.7 billion) was blamed on business email compromise.
The RIG exploit kit, one of the most successful malvertising tools to hit the internet, takes the split seconds it takes for an ad to redirect to its intended location to inject malware into a browser commanding it to begin encrypting files that can then be held for ransom.

MALVERTISING
That Ad Isn’t What You Think It Is

This type of phishing takes advantage of exploits within advertising or animation software to steal information from targeted users. Malvertising is usually embedded in otherwise normal-looking ads—and placed on legitimate websites like Yahoo.com—but with malicious code implanted within.

A Nasty Surprise

The Angler exploit kit (shown below) famously delivered CryptXXX, a previously ubiquitous ransomware that generated $3 million per month for its creators.
HOW TO PROTECT YOURSELF FROM PHISHING ATTACKS

Protecting yourself from phishing attacks starts with knowing what’s out there. In fact, according to Webroot research, ongoing security awareness training can help reduce breaches by nearly 70%.

Here are a few tips to keep in mind to avoid getting phished:

1. Never click on links from unknown senders or if any detail about the exchange has aroused suspicion.

2. Whenever possible, hover over a link to ensure the destination matches your expectations. Note this will not work on mobile or if short codes are used, so be extra wary on mobile devices.

3. If you suspect an email is a phishing attempt, double check the sender name, specificity of the salutation, and a footer for a physical address and unsubscribe button. When in doubt, delete.

4. If you’re unsure if a communication is legitimate, try contacting the brand or service via another channel (their website or by calling a customer service line, for instance).

5. Avoid entering personally identifiable information unless you are extremely confident in the identity of the party you are communicating with.

Closing All Your Security Gaps

While staying vigilant will keep most attackers at bay, no one can be 100% secure on their own. After all, phishing only exists today because it works. This is why it’s important to combine security awareness training with quality business endpoint protection—with AI-enhanced threat intelligence, cloud-based updates, and real-time anti-phishing—DNS protection, and reliable data backup.

By implementing one, two, or all five of the above solutions, you can rest easier that your business is more resilient against this growing threat.
Protect your business.
Protect your livelihood.

BECOME CYBER RESILIENT.

Webroot and Carbonite together offer best-in-class endpoint security and enterprise-grade backup and recovery in a comprehensive suite built for businesses like yours. Start with our award-winning endpoint protection.

GET STARTED