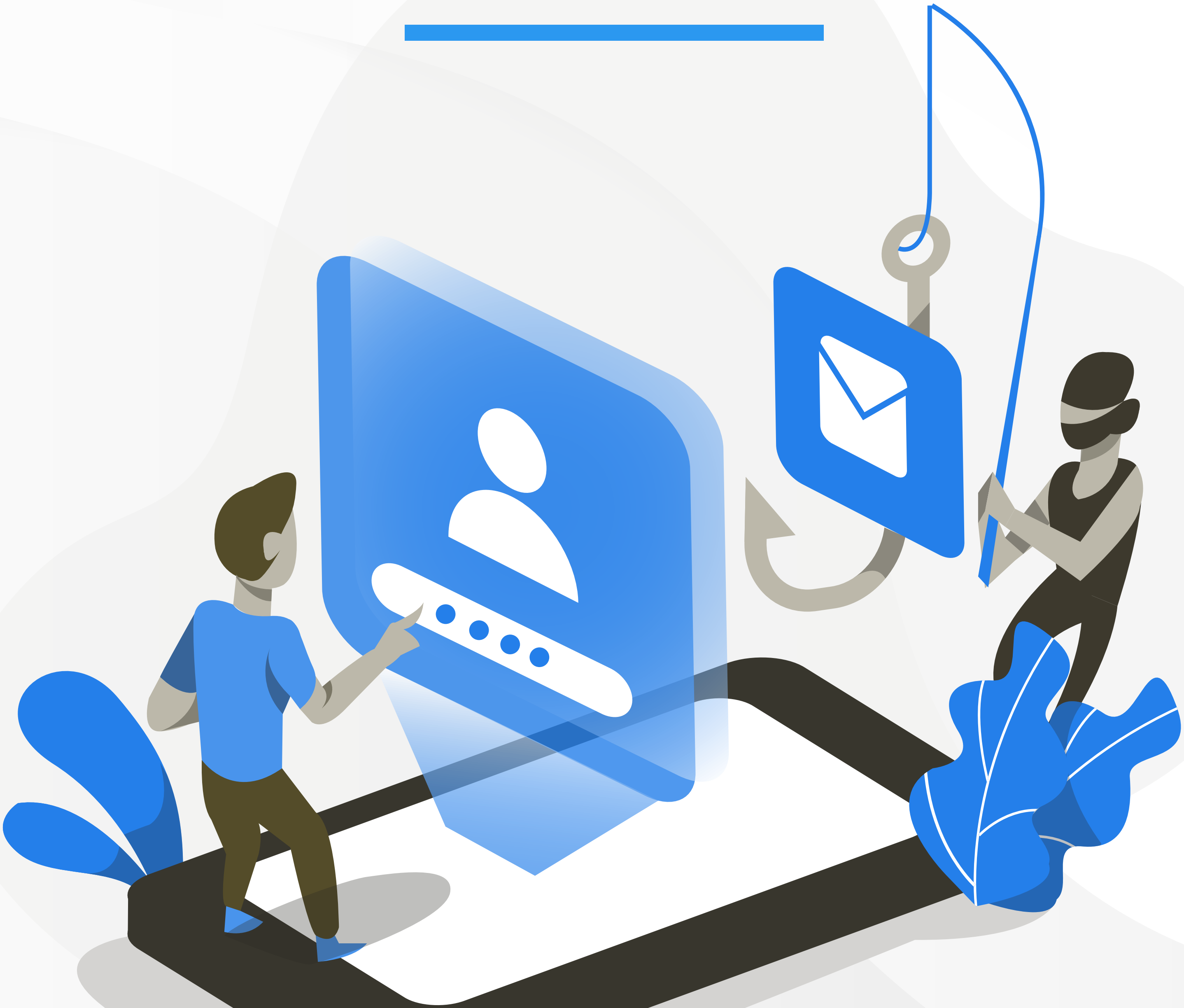
THE PRICE OF PHISH

What You Need To Know About Phishing



DNSFilter

What You Need To Know About Phishing

When it comes to phishing scams, there are plenty to go around. You get a phishing email and you get a phishing email. Everyone, everywhere, of all ages gets a phishing email.

But it's possible that you've gotten a phishing email without realizing that's what it was. In this whitepaper we'll cover what a phishing scam is (with 6 examples), trends to look for that indicate you've found a phishing scam, who's at risk, and how to mitigate attacks.

What is phishing?

A phishing attack is when a malicious party lures someone into taking a specific action (usually handing over money or valuable credentials) through false pretenses.

It shouldn't be a surprise, but the term "phishing" is a play in "fishing." So in a sense, hackers are casting a line and waiting to see who gets hooked.

They do this by setting up deceptive websites or sending out an email to intentionally misguide someone into handing over their information.

This can take many forms, but these are a few major examples:

The not-your-real-login login page

This is when a page looks like a login you use all the time, but in reality it's a phishing scam. Duplicating Office 365 login pages is a common tactic that hackers use.

The key is looking at the URL of the page for anything *fishy*.

The donate-to-a-good-cause charity website

Unfortunately, hackers are very eager to take advantage of people's desire to support good causes. They do this by setting up *fake* causes for you to care about and donate to. Most often, they utilize recent tragedies getting a lot of coverage in the news. Then, they'll set up a page claiming that any funds you donate will go to help the cause you care about.

What these hackers *really* want are your login credentials.

The I'm-your-uncle's-neighbor-and-he's-in-trouble message

Who's gotten this one? Someone you love is in the hospital and you need to wire some money or share bank account details in order to make sure they get an operation. Or, they're wrongfully in jail and they need to make bail.

All you need to do is send a few Bitcoin their way. And of course you can't actually call your uncle, he's indisposed.

This type of scam is a growing Vishing (voice-phishing) trend, but you'll still find it via email.

If you find yourself in the middle of a scam trying to take advantage of you caring about your loved ones, do yourself a favor and *actually call them* before you send any money anywhere.

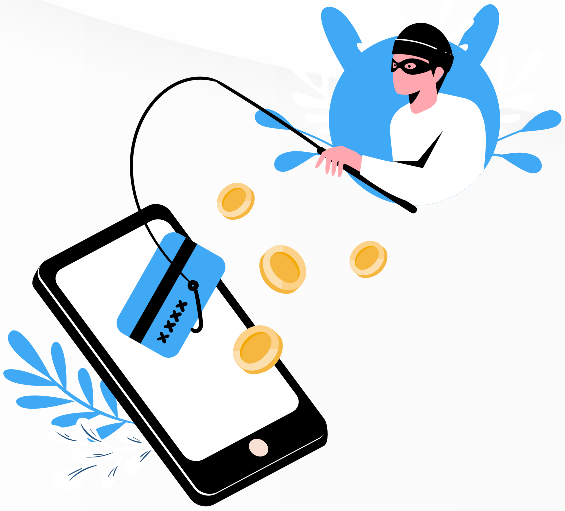
The your-boss-needs-your-help email forward

This tactic seems to be most successful, and it's one I've seen firsthand in my own inbox.

The email might come from someone you don't know, but the body of the email will have a long email forward that includes a message from your boss expressing that they need money wired to them and it is urgent. The person will usually claim to be a friend or relative of your boss and supply you with a link so that you can wire possibly *thousands of dollars* to your boss.

An alternate version of this email omits the forward completely and is sent from an email attempting to mimic your boss' email. This is done by either creating a Gmail account with your boss' name in it, or even registering a domain that is *similar to your company's* domain. So if I were to receive a message from "ken@dnsfltr.scam", I might think it's from our CEO at first-glance.

Well, if "scam" is in the address, I hope I don't fall for *that* one.



The there-is-a-problem-with-your-bank-account urgent email

Another favorite tactic of scammers. *Everyone* pays attention when it comes to their bank account being in jeopardy. So if you get an email claiming that you need to take action in the form of transferring money from your account, double-check that email.

These types of scams usually have "bank" in the sender address. But if it doesn't match the name of your current bank, do not click *anything* in that email. Even if it does, call your bank first and talk to them.

The ERROR-you've-downloaded-a-virus-here's-how-to-fix-it popup

There's nothing scarier than seeing a message that you've downloaded a virus on your computer. A million things can enter your mind: What have they taken? What files are ruined? And most importantly *How do I fix it*?

That last question is where the hackers hope your mind goes *first*. They set up these pop-ups hoping that you'll immediately pay (without thinking about it) to stop the virus from spreading. Of course, there is no virus.

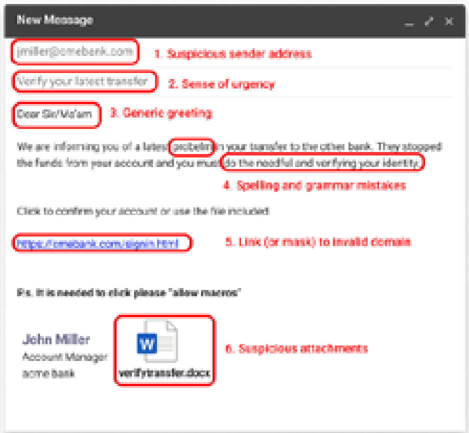
This technique is basically the lazy hacker's ransomware alternative. They don't want to actually go through the trouble of encrypting all your files and asking you to pay a ransom. They just want you to *think* everything is inaccessible.

Navigate away if you run into this type of malicious webpage. And please do not pay the $20 to fix your computer when your computer isn't even broken.

What do these attacks **have in common?**

A few commonalities you'll find in a lot of phishing schemes are:

- Typos *everywhere*
- Strange spelling and grammar
- inks displayed are different from the actual links (you can confirm this out by hovering your cursor over a link)!
- Suspicious email senders
- Suspicious email attachments
- Emails don't address you by name ("Sir/Madam" instead of "Serena")



New Message

jmiller@omebank.com

Verify your latest transfer

Dear Sir/Ma'am

We are informing you of a latest probelm in your transfer to the other bank. They stopped the funds from your account and you must do the needful and verifying your identity.

Click to confirm your account or use the file included

https://omebank.com/signin.html

P.s. It is needed to click please "allow macros"

John Miller
Account Manager
acme bank

verifytransfer.docx

1. Suspicious sender address

2. Sense of urgency

3. Generic greeting

4. Spelling and grammar mistakes

5. Link (or mask) to invalid domain

6. Suspicious attachments

Why do we keep finding these trends **among phishing attacks?**

There are a few reasons.

First, hackers don't want to waste their time with people who will spot a scam that doesn't even have typos to begin with. These are usually more technical folks or people who are well-versed in what a scam looks like. These people can cause a lot of headache for scammers by toying with them (being the troll) and leading the hacker into a long, drawn-out conversation.

When a message has enough typos and actually looks like spam, people using spam blockers will likely never see the email. And that's not who hackers want. They want the people who don't even know spam blockers exist.

Second, generalizing the message allows hackers to send the messages to thousands of people at once. While hackers could go through the work of personalizing these emails, it doesn't really behoove them to do so since the people they're looking to target wouldn't care about those types of details anyway.

Third, the sense of urgency is very important in these matters. They want people to react quickly without thinking. Hackers are banking on people to respond emotionally instead of logically.

Finally, links will always be made to look like one thing (bankofamerica.com) but actually point to somewhere else (westealyourmoney.scam). The reason for this is pretty obvious. They want you to think that you're heading to a real bank account login, a bail bonds website, a hospital, or a Microsoft page. If they show their hand, you're more likely not to click on that link.

Why is phishing such **a popular method for hackers?**

Phishing attacks are easy to deploy. If you've seen some of these emails, you probably understand that they're low effort. Once they have the links where people can hand over bank account information or online logins, they can send blasts. A lot of their attempts get filtered through spam detectors, but enough get through those detectors that it's worth their while.

It's also worth noting that a single phishing attack can result in a huge payout. Barbara Corcoran fell for a scheme and paid over $400,000. Mattel nearly lost $3 million in 2015 to a phishing scam, but luckily because of bad-timing on the part of the hacker, they were able to recoup that money. Over a period of a few months, the European theater chain Pathé lost nearly $21 million because they were unknowingly wiring money to fraudsters.

The big takeaway here is that there are a variety of phishing scams that hackers can deploy depending on how dedicated they are to the scam. And it's proven time and again that these scams work.

Who is the **main target** of a phishing scam?

According to Knowbe4, 1 in 3 employees are likely to click a malicious link or obey a request that turns out to be fraudulent. Employees in the following industries are awarded the superlative "most-likely-to-fall-for-a-phishing-attack":

Healthcare

Construction

Government

Finance

Hackers can launch hyper-targeted campaigns, aiming to steal money from major companies using phishing attacks. Or, they can set up a more generic phishing scheme in an attempt to get smaller payouts from a wide range of people.

Phishing scams are always a one-on-one scam, meaning it's the *hacker* talking to the *victim*. Emails may be deployed en masse, or pages viewed by multiple people, but for the hacker it's always about convincing a single person to click that link and fork over information (or money).

And that pretty much means *everyone* can be the target of a phishing scam. Though midsized companies are at serious risk of falling victim to well-organized (and costly) phishing attacks.

Attacks targeting specific companies are called "spear phishing" attacks.

The reason for targeting a certain company could be as simple as they were able to procure an email list from that company. Other reasons might be knowledge of a company's funding status or new personnel so that they can address recent changes when pretending to be someone inside the company.

But the fact that anyone can be the target of a phishing attack doesn't mean you should be afraid to open your email or click on links everytime you open your computer. What it does mean is that you should be careful online. Knowing that these phishing attacks are out there is the first step.

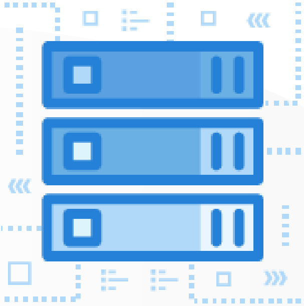
How can I stop **Phishing Attacks?**

Educate yourself & your team

Education is a *huge* factor in minimizing the number of people who fall for phishing scams. But part of the reason these scams work is because the hackers that deploy these attacks are clever. So educating your employees is step No. 1 in prevention. Tell them what to look for.

Use a **password manager**

Your password manager won't recognize a fake login page, so it won't give you the option to enter your Microsoft password on actuallynotmicrosoft.com. This can really help you out when you're in a hurry.



Adopt a **DNS solution.**

This takes the responsibility of determining if something is a threat or not out of the hands of your employee. If DNS protection software deems a site is a phishing website, it will not allow you to view the page. If you're sent a phishing email asking you to transfer money, it won't open any links you click within the email. Advanced DNS solutions will also use domain greylisting, which blocks newly registered domains for 30 days. This is invaluable as a majority of phishing sites are brand new.

To keep your staff from becoming another victim of phishing attacks, you need to put security in place to protect them.

Get your free trial of DNS Protection

Who is DNSFilter

DNSFilter is DNS security that protects your entire organization from online security threats and undesirable content, including phishing attacks. With powerful artificial intelligence and an industry-leading global network behind DNSFilter, you can be safe and secure from internal risks and external threats in mere minutes.