SECURITY GUIDE

The McAfee Safety Series

Phishing Protection Guide

Table of Contents

Phishing. A leading form of cybercrime.

What makes phishing so popular with scammers and thieves? It's effective.

Whether it comes by way of email, text, instant message, or direct message on social media, a phishing attack plays on one of our greatest vulnerabilities—our emotions. With a phony message that looks like it comes from a business, bank, government organization, or even a friend, scammers will play off your sense of trust, not to mention a host of emotions that can range anywhere from excitement to fear.

That's what can make a phishing attack so effective.

Some examples ...

- "You've won our cash prize drawing! Send us your banking information so we can deposit your winnings!"
- "You owe back taxes. Send payment immediately using this link or we will refer your case to law enforcement."
- "We spotted what may be unusual activity on your credit card. Follow this link to confirm your account information."

Throw in a couple logos or two and plenty of people might find themselves tempted to click the link that comes along with that message.

However, it's a scam. Designed to separate you and your money, personal information, or both.

How do phishing attacks work?

Phishing, as its name implies, takes a bait-and-hook approach to trick people out of their personal information, account logins, and even their data. The bait comes in the form of a message where scammers will reach out under the guise of a legitimate business, organization, or perhaps as someone the victim knows.

Once someone takes the bait, the scammer attempts to set the hook. Sometimes that involves a link to a phony login page where they can steal account credentials, other times scammers will use malware that can install all kinds of trouble on a device—like keylogging software that steals information, viruses that open a back door through which data can get hijacked, or ransomware that holds a device and its data hostage until a fee is paid.

The tricky thing with phishing attacks is that they can be tough to spot. It used to be that phishing attacks were typically clumsy looking. You could point to misspellings, lousy grammar, poor design, and logos that looked stretched or that used the wrong colors. Poorly executed phishing attacks like that still make their way into the world, yet it's increasingly common to see far more sophisticated attacks that appear like a genuine message or notice.

Phishing takes a bait-and-hook approach to trick people out of their personal information, account logins, and even their data.

Let's look at three examples of phishing attacks that scammers have launched under our name:

There's a lot going on in this first example. The scammers try to mimic the McAfee brand, yet don't quite pull it off. Still, they do several things to try and be convincing.

Note the use of photography and the box shot of our software, paired with a prominent "act now" headline. It's not the style of photography we use. Not that people would generally know this. However, some might have a passing thought like, "Huh. That doesn't really look right for some reason."

Beyond that, there are a few capitalization errors, some misplaced punctuation, plus the "order now" and "60% off" icons look rather slapped on. Also note the little dash of fear it throws in with mention of "There are (42) viruses on your computer ..."

Taken all together, someone can readily spot that this is a scam with a closer look, seeing what doesn't feel right about the ad, and then trusting their gut.

This next ad falls into the less sophisticated category. It's practically all text and goes heavy on the red ink.

Once again, it hosts plenty of capitalization errors, along with a few gaffes in grammar as well. In all, it doesn't read smoothly. Nor is it easy on the eye, as a proper email about your account should.

What sets this example apart is the "advertisement" disclaimer below, which attempts to lend the attack some legitimacy. Also note the phony "unsubscribe" link, plus the (scratched out) mailing address and phone, which all attempt to lend an air of legitimacy.

This last example doesn't get our font quite right, and the trademark symbol is awkwardly placed. The usual grammar and capitalization errors crop up once again, yet this piece of phishing takes a slightly different approach.

The scammers placed a little timer at the bottom the email. That adds a degree of scarcity. They want you to think that you have about half an hour before you are unable to register for protection. That's absolutely bogus of course.

Seeing any recurring themes? There are a few for sure. With these examples in mind, get into the details—how you can spot phishing attacks and how you can avoid them altogether.

How to spot and prevent phishing attacks

Just as we saw, some phishing attacks indeed appear fishy from the start. Yet sometimes it takes a bit of time and a particularly critical eye to spot.

And that's what scammers count on. They hope that you're moving quickly or otherwise a little preoccupied when you're going through your email or messages—enough so that you may not pause to think, *Is this message really legit?*

One of the best ways to beat scammers is to take a moment to scrutinize that message while keeping the following in mind …

Spotting phishing attacks

They play on your emotions

Fear. That's a big one. Whether it's an angry-sounding email from a government agency saying that you owe back taxes or a text from a family member asking for money because there's an emergency, scammers will lean heavily on fear as a motivator.

If you receive such a message, think twice. Consider if it's genuine. For instance, consider that tax email example. In the U.S., the Internal Revenue Service (IRS) has specific guidelines as to how and when they will contact you. As a rule, they will most likely contact you via physical mail delivered by the U.S. Postal Service. (They won't call or apply pressure tactics—only scammers do that.) Likewise, other nations will have similar standards as well.

They tell a whopper of a story

Whether it's word of an unexpected windfall from a sweepstakes you haven't heard of—or the notorious example of the prince who needs your help to shuffle his fortune from one bank to another—scammers love to spin one heck of a tale. Just crazy enough for you to think it could be possible.

Put plainly, if you receive a message that leaves you scratching your head after you read it, chances are it's a scam. Delete it and move on.

They ask you to act—NOW

Scammers also love urgency. Phishing attacks begin by stirring up your emotions and getting you to act quickly. Scammers may use threats or overly excitable language to create that sense of urgency, both of which are clear signs of a potential scam.

Granted, legitimate businesses and organizations may reach out to notify you of a late payment or possible illicit activity on one of your accounts, yet they'll take a far more professional and even-handed tone than a scammer would. For example, it's highly unlikely that your local electric utility will angrily shut off your service if you don't pay your past due bill *immediately*.

They want you to pay a certain way

Gift cards, cryptocurrency, money orders—these forms of payment are another sign that you may be looking at a phishing attack. Scammers prefer these methods of payment because they're difficult to trace and offer consumers little to no way of recovering lost funds once they're sent.

Legitimate businesses and organizations will not ask for payments in those forms. If you get a message asking for payment in one of those forms, you can bet it's a scam.

They use mismatched addresses

Here's another way you can spot a phishing attack. Take a close look at the addresses the message is using. If it's an email, look at the email address. Maybe the address doesn't match the company or organization at all. Or maybe it *kind of* does, yet adds a few letters or words to the name. This marks yet another sign that you may have a phishing attack on your hands.

Likewise, if the message contains a web link, closely examine that as well. If the name looks at all unfamiliar or altered from the way you've seen it before, that could also mean you're looking at a phishing attempt.

How to avoid phishing attacks

Go directly to the source

Some phishing attacks can look convincing. So much so that you'll want to follow up on them, like if your bank reports irregular activity on your account or a bill appears to be past due. In these cases, don't click on the link in the message. Go straight to the website of the business or organization in question and access your account from there. Likewise, if you have questions, you can always reach out to their customer service number or web page.

Don't download attachments

Some phishing attacks involve attachments packed with malware like the ransomware, viruses, and keyloggers we mentioned earlier. Scammers may pass them off as an invoice, a report, or even an offer for coupons. If you receive a message with such an attachment, delete it. And most certainly don't open it.

Even if you receive an email with an attachment from someone you know, follow up with that person. Particularly if you weren't expecting an attachment from them. Scammers will often hijack or spoof email accounts of everyday people to spread malware.

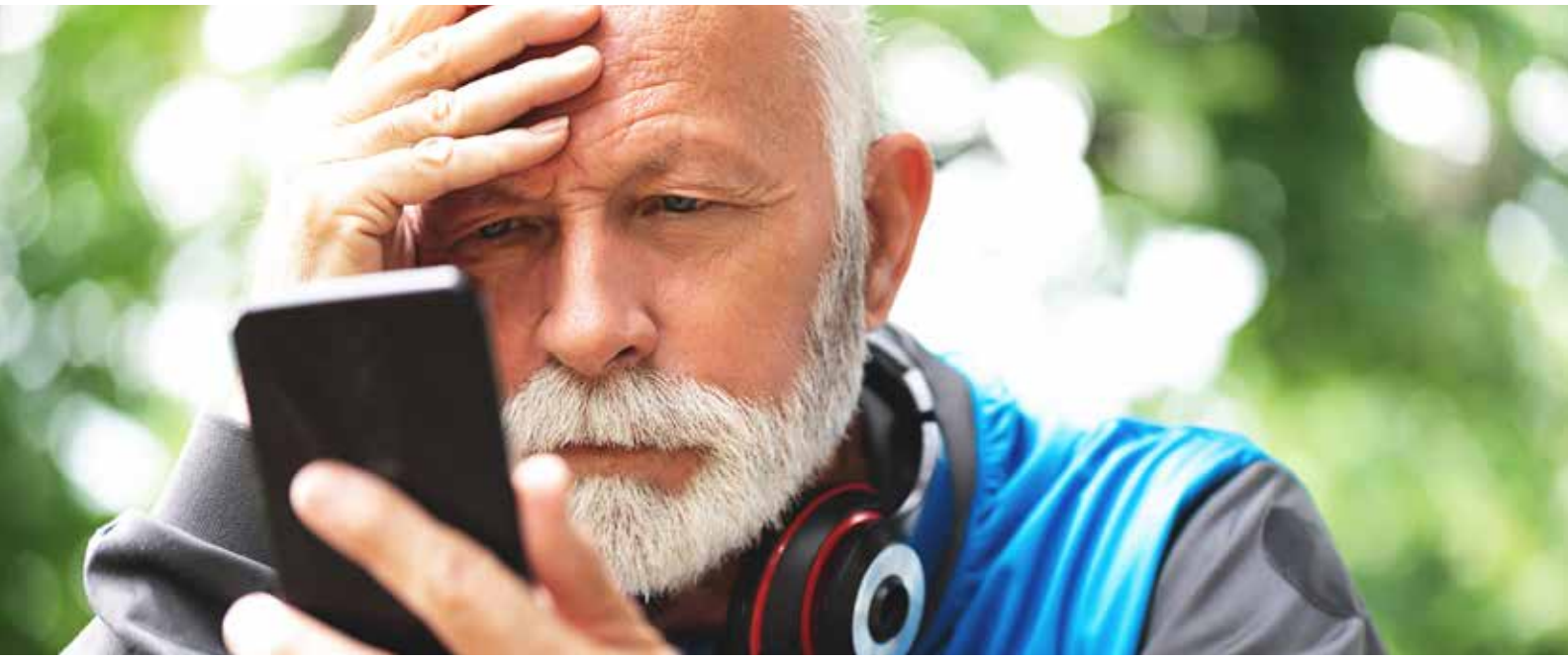
Hover over links to verify the URL

On computers and laptops, you can hover your cursor over links without clicking on them to see the web address. If the URL looks suspicious in any of the ways we mentioned just above, delete the message and don't ever click.

Use online protection software

Online protection software can protect you in several ways. First, it can offer safe browsing features that can identify malicious links and downloads, which can help prevent clicking them. Further, it can steer you away from dangerous websites and block malware and phishing sites if you accidentally click on a malicious link. And overall, strong virus and malware protection can further block any attacks on your devices.

Be sure to protect your smartphones in addition to your computers and laptops as well, particularly given all the sensitive things we do on them, like banking, shopping, and booking rides and travel.



I fell for a phishing scam. What should I do now?

Despite our best intentions and efforts, mistakes happen—like clicking on a phishing link or handing over some personal info to a bogus site.

The first order of business is to keep cool. Next, get to work quickly so you can minimize or prevent any damage.

1. Reset your passwords. If you shared any account information, immediately create a new password for that account, one that's strong and unique. (You may consider using a password manager to do that work for you on all your accounts. Online protection software often includes one. Some are free as well, like our own McAfee True Key™.)

2 .Reach out to the company or institution involved. Let them know that your account info may have been stolen as part of a phishing attack. Many organizations have a consumer fraud department and consumer fraud policies that can assist you.

3. Also, report the attack to your government's fraud or trade agencies. In the U.S., the identity theft website from the Federal Trade Commission (FTC) is a fantastic resource should you find yourself in need. In addition to keeping record of the theft, the FTC can provide you with a step-by-step recovery plan—and even walk you through the process if you create an account with them.

You can also report scams involving malware, fake websites, and phishing attacks to the Internet Crime Complaint Center (IC3).

Other nations have similar resources available as well:

- In the UK; https://www.actionfraud.police.uk/
- In Ireland: https://www.garda.ie/en/crime/fraud/
- In Canada, https://www.antifraudcentre-centreantifraude.ca/
- In Australia, https://www.counterfraud.gov.au/find-where-report-fraud/
- In New Zealand, https://sfo.govt.nz/

4. Monitor your credit and identity. Phishing attacks can often lead to identity theft. Many attacks are designed specifically for identity theft purposes, such as bogus websites that steal credit card info, logins to social media sites, and other financial accounts.

To protect yourself, strongly consider using a credit and identity monitoring service. The reality is that one phishing attack can lead to several follow-on attempts at identity fraud and theft. Identity monitoring like McAfee's can keep tabs on potential misuse of your email addresses, Social Security Number, bank accounts, credit cards and more. If we detect a change, you'll be alerted up to an average of 10 months sooner before our competitors.

Likewise, depending on your location and plan[1], McAfee's credit monitoring can help you look after your credit score and accounts to see fluctuations and identify unusual activity so you can determine if it was unauthorized. Identity theft protection further offers financial coverage for losses and expenses, in addition to hands-on help from a recovery professional, to help restore your identity.

For more on protecting yourself from identity theft, check out our security guide on identity theft protection. As you can imagine, it's an entire topic of its own, and our guide covers it in detail.

1. Legal statement regarding plans and availability

So many phish in the sea

No doubt about it, scammers love phishing attacks—because they're so effective.

By playing on your emotions, adding in a sense of urgency, and simply doing their best to look legitimate, scammers hook millions of victims a year with phishing attacks. One study concluded that one in every 99 emails is a phishing attack—and that more than half contained malware and some 40% were designed to steal credentials.

Clearly, phishing attacks present a major hazard to people and their families, which makes knowing what to look for and how to avoid them in the first place so important. A combination of a sharp eye and online protection software offer a terrific defense, just as we covered above. So does trusting your gut. If something doesn't look or sound right, chances are it isn't. Delete that message and go on your way. And smile when you do. You just beat a scammer at their game.

Protecting yourself further

For more on protecting yourself from phishing attacks and online protection overall, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2022 McAfee, LLC. AUGUST 2022