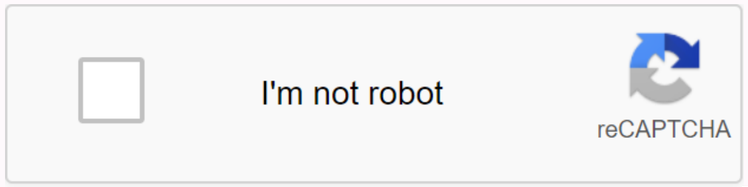

Continue

Apple spoof email forwarding

Even if you've never been the victim of a phishing attack, you may have seen an attempt - an email from Apple or Google asking you to update your account information, or a Nigerian prince seeking money to return him to the throne. But while phishing baits may be quite obvious, there are others that may be a little harder to identify. Fortunately, there are plenty of signs you can look to determine if someone is trying to accidentally get important credentials from you. Here's how you might be able to identify phishing attacks, and how to report them. What is phishing? Most basic, phishing is when someone tries to get information like passwords and credit card numbers by posing as someone you might trust. Attackers will often spoof legitimate websites, for example, Apple, and try to guide their targets to that location in an attempt to access some sort of credential. While phishing attacks generally occur via email, attackers are also known to use other methods such as instant messaging and phone calls. How do I identify phishing scams? The most common type of phishing scam is trying to try and retrieve your password and username through social engineering. These attacks are often disguised as emails from large companies such as Apple, Google, Facebook, or your bank; mostly, that's because these companies have millions of customers and the opportunity to email someone who actually uses the service from that website is very high. These emails will contain links to pampered websites masquerading as legitimate corporate pages, usually asking you to log in or ask security questions. There are a few different things you can do that can help you identify if you are the target of a phishing attack. Note that you should not rely solely on one of these techniques to identify phishing scams; Sophisticated attackers work hard to pass their scams (and related websites) as legitimate, and seeing scammers can be more difficult than they first appear. Go with your gut First advice is also the most technical. If you feel completely suspicious about an email, don't click at all. Also reach out to the person or company that sent you the message (with the original message, don't reply to the message you just received) and ask if they're sending you something. The subject of an email disguised as a legitimate company, an attacker will often ask you to do something like verify your password or update your account information. Most legitimate companies, banks, and other institutions will not ask for account details via email or SMS. Check the address (and link) you should see the email address of the messages you receive, which you can often do by clicking (or tapping) their display name (another thing to prepare). If an email address is strange, or seems too long for the company is a question, don't trust that email. However, a smart attacker will including the company name somewhere in the email address in an attempt to appear more legitimate. It's important to pay attention to the legitimate email your bank uses, for example, sending you, and what email address or address they use. This also applies to the links they send you. Without clicking on the link, hover your mouse over it or tap and hold the link on your mobile device for more details. If it doesn't look like a link from a company, it might not. It's also a good idea to check the email address where the message has been sent. For example, I often receive emails from Google, but they've been sent to my iCloud email address instead of the backup email addresses I've set up with Google. Check the names While many attackers can easily spoof company names in their phishing attempts, less sophisticated attacks will get even these details wrong. Others will use names that may seem correct at first glance, but on closer inspection contain errors. For example, a recent attempt I saw was sent by AppleID Support. This name has some red flags. For one, Apple spells it apple ID with spaces. Second, Apple emails are often sent from Apple, without certain branding such as Support. Spelling and grammar materials Are just as strange as some, spelling and grammar can often provide phishing attempts. Someone I know recently received an email with this phrase: We've prevented unusual activity on your account. Someone logged in and reset your password. Things like this are a dead giveaway. In this case, the email came from AppleID Support, and there were some pretty obvious errors in grammar. Check the style Be sure to pay attention to the style of the email sent to you. Get a Google email whose color or logo looks a little outdated? That might be a scam, for example. Companies almost always have contact details or at least addresses at the bottom of emails, while many phishing emails don't. The Federal Trade Commission maintains a Fraud Alert website that warns consumers of the dangers of phishing attacks. The site offers news about new attacks, as well as general newsletters on online security and avoiding fraud. Use all this The thing about avoiding phishing is that it's not about one technique. Attacks can be very incompetent or very sophisticated. It's important to be careful, and not put all your trust in one solution. How do I report phishing? There are a number of resources you can use to report phishing attempts, both to the company and to the government. Companies such as Apple and Facebook often have dedicated email addresses to forward phishing attempts, while Google has buttons in Gmail that You did just that. When using the following link, be sure to forward the phishing email you reported: I've been the victim of a phishing scam. What am I supposed to do? Contact a company whose credentials are credentialed phished, and see what they can do to help you. If the attacker gets your credit card, be sure to cancel the card. As soon as you can, you'll also want to reset any passwords you need. Questions? If you want to know anything else about phishing, or even relay phishing attacks or attempts that have occurred to you, be sure to sound off in the comments. Updated January 2019: We have updated this section with the latest information in light of the latest phishing scams. We may earn commissions for purchases using our links. Learn more. Fraudsters use email or text messages to trick you into giving them your personal information. But there are a few things you can do to protect yourself. Fraudsters use email or text messages to trick you into giving them your personal information. They can try to steal your password, account number, or Social Security number. If they get that information, they can get access to your email, bank, or other account. Fraudsters launch thousands of phishing attacks like this every day - and they often succeed. The FBI's Internet Crime Complaint Center reports that people lost $57 million to phishing schemes in one year. Scammers often update their tactics, but there are some signs that will help you recognize phishing emails or text messages. Phishing emails and text messages may look like they're from companies you know or trust. They may look like they come from banks, credit card companies, social networking sites, websites or online payment apps, or online stores. Phishing emails and text messages often tell stories to trick you into clicking on links or opening attachments. They may say they've seen some suspicious activity or attempted log-ins claiming there's a problem with your account or your payment information says you should confirm some personal information including a fake invoice wanting you to click a link to make a payment saying you're eligible to sign up for a government refund offering coupons for free stuff Here's a real-world example of phishing emails. Imagine you see this in your inbox. Do you see any signs that it is a scam? Let's see. The email appears to come from a company you may know and trust: Netflix. It even uses the Netflix logo and header. The email says your account was suspended due to billing issues. The email has a generic greeting, Hi Dear. If you have an account with a business, it probably won't use generic greetings like this. The email invites you to click the link to update your payment details. While, at a glance, this email may look real, it The fraudsters who send emails like this have nothing to do with the company they're pretending to be. Phishing emails can have real consequences for people who give their information to fraudsters. And they can jeopardize the reputation of their corporate spoofing. How to Protect Yourself From Phishing Attacks Your email spam filter may keep many phishing emails out of your inbox. But scammers are try outsmarting spam filters, so it's a good idea to add an extra layer of protection. Here are four steps you can take today to protect yourself from phishing attacks. 1. Protect your computer by using security software. Set the software to update automatically so that it can handle new security threats. 2. Protect your phone by setting the software to update automatically. This update may provide you with critical protection against security threats. 3. Protect your account by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to sign in to your account. This is called multi-factor authentication. The additional credentials you need to sign in to your account fall into two categories: Something you have – such as a passcode you get via text message or an authentication app. Something you are - like scanning your fingerprint, your retina, or your face. Multi-factor authentication makes it harder for fraudsters to log into your account if they get your username and password. 4. Protect your data by backing it up. Back up your data and make sure it's not connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone as well. What To Do If You Suspect a Phishing Attack If you get an email or text message asking you to click a link or open an attachment, answer this question: Do I have an account with the company or know the person who contacted me? If the answer is No, it could be a phishing scam. Go back and review tips in How to recognize phishing and look for signs of phishing scams. If you see it, report the message and delete it. If the answer is Yes, contact the company using a phone number or website that you know is real. Not the information in the email. Attachments and links can install malicious malware. What To Do If You Respond to Phishing Emails If you think fraudsters have your information, such as Social Security, credit cards, or your bank account number, go to IdentityTheft.gov. There you'll see specific steps to take based on lost information. If you feel like you clicked a link or opened an attachment that downloaded malicious software, update your computer's security software. Then run the scan. How to Report Phishing If you get a phishing email or text message, report it. The information you provide can help fight scammers. Step 1. If you have phishing emails, forward them to the Anti-Phishing Working Group reportphishing@apwg.org. If you get a phishing text message, forward it to SPAM (7726). Step 2. Report phishing attacks to the FTC in ftc.gov/complaint.