Learn about the Adversary-in-the-Middle phishing attack method

Phishing attacks are extremely common right now. This method of cybercriminals can be very effective in stealing data and does not require a large amount of work at the grassroots level.

However, phishing also comes in many forms, one of which is the Adversary-in-the-Middle phishing attack. So, what are the Adversary-in-the-Middle phishing attacks? And how can you avoid them?

What is an Adversary-in-the-Middle Attack?

An Adversary-in-the-Middle (AiTM) phishing attack involves stealing session cookies to steal personal data and even bypassing authentication layers.

You may have heard of cookies before. Today, most of the websites that you click on will ask you for permission to use cookies to better tailor your online experience. In short, cookies track your online activity to understand your habits. They are small text files of data that can be sent to your server every time you click on a new web page, thus giving certain parties the ability to monitor your activity.

There are many types of cookies. Some are necessary, and some are simply not. AiTM attacks involve session cookies. These are temporary cookies that store user data during a web session. These cookies are lost immediately after you close your browser.

As often happens in phishing, an AiTM phishing attack begins with the cybercriminal communicating with the target, usually via email. These scams also use malicious websites to steal data.

AiTM attacks are a particularly pressing issue for Microsoft 365 users, with attackers communicating with their targets and asking them to sign in to their 365 accounts. The malicious person will impersonate an official Microsoft address in this phishing attack, which is also typical in phishing attacks.

The goal here is not just to steal credentials but to bypass the victim's multi-factor authentication (MFA) or two-factor authentication (2FA) layer. These are security features used to verify account logins by requesting permissions from a separate device or account, such as your smartphone or email.

Cybercriminals will also use proxy servers to communicate with Microsoft and host a fake 365 login page. This proxy allows an attacker to steal the victim's session cookie and credentials. When the victim enters their credentials into the malicious website, it steals the session cookie to provide false authentication. This gives attackers the ability to bypass the victim's 2FA or MFA request, granting them direct access to their account.

How to protect against AiTM phishing attacks

Picture 1 of Learn about the Adversary-in-the-Middle phishing attack method

Although the AiTM phishing attack is different from a regular phishing attack, you can still use the same methods to avoid it.

Start with any of the links provided in your email. If you receive an email from a supposedly trusted sender saying that you need to use the link provided to log into one of your online accounts, proceed with caution. This is a classic phishing trick and can trap many victims, especially if the attacker uses persuasive or urgent language urging the target to log into the account as soon as possible.

So, if you receive an email that includes any kind of link, make sure you run it through a link-checking site before clicking. On top of that, if the email says you need to sign in to your account, just search for the login page in your browser and access your account there. This way you can see if there are any issues you need to solve on your account without clicking on any kind of provided links.

You should also avoid opening any attachments sent to you from an unfamiliar address, even if the sender claims to be a trusted individual. Malicious attachments can also be used in AiTM phishing attacks, so you need to be wary of what you open.

In short, if there's really no need to open the attachment, just leave it at that.

On the other hand, if you need to open attachments, do some quick tests before doing that. You should look at the file type of the attachment to determine if it is considered suspicious. For example, .pdf, .doc, zip and .xls files are known to be used in malicious attachments, so be wary if the attachment is one of these file types.

Above all, check the context of the email. If the sender claims that the attachment contains material, such as a bank statement, but the file has the .mp3 extension, you may be dealing with a phishing and potentially dangerous attachment, because the file MP3 will not be used for the document.

Picture 2 of Learn about the Adversary-in-the-Middle phishing attack method

Check the sender address of any suspicious emails you receive. Of course, every email address is unique, so an attacker can't use the company's official email address to contact you, unless it's hacked. In the case of phishing, attackers often use email addresses that look a bit like the official address of the organization.

For example, if you receive an email from someone claiming to be Microsoft, but you notice that the address says "micr0s0ft" instead of "Microsoft", you are experiencing an online scam. Criminals will also add an additional letter or number to the email address so that it looks a lot like the legitimate address.

You can even determine if a link is suspicious by looking at it. Malicious websites often have links that look unusual. For example, if an email says the provided link will take you to Microsoft's login page, but the URL says this is a completely different website, it's clearly a hoax. Checking a website's domain can be especially helpful in preventing phishing.

Finally, if you receive an email from a supposedly official source with lots of spelling and grammar errors, you may be being scammed. Official companies often ensure that their emails are written correctly, while cybercriminals can sometimes be sloppy in this regard. So, if the email you receive is sloppy, be wary of any action you take next.

Phishing is very common and is used to target both individuals and organizations, meaning that no one is really safe from this threat. So to avoid AiTM phishing attacks and phishing in general, consider the tips provided above to keep your data safe.

You finished reading the article "**Learn about the Adversary-in-the-Middle phishing attack method**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
