RATE HAWK

Phishing Awareness: How to Protect Your Account from Online Threats

Have you ever received suspicious emails urging you to follow a link? There is a high chance that it was phishing. To safeguard your data and stay ahead of potential threats, being aware and taking proactive measures are paramount. In this article, we will delve into effective steps for your cybersecurity and explore what measures to take when working with our platform.

1 Phishing in Figures: Understanding the Threat

15%

of all data breaches are due to phishing (IBM report).

$52M+

in losses reported due to phishing in the US (FBI IC3, 2022).

300k

victims reported in the US in 2022.

Phishing attacks are increasing, threatening individuals and businesses worldwide. According to IBM's report, phishing is the most common data breach vector, accounting for 15% of all breaches. The financial toll is just as alarming — figures from the FBI's Internet Crime Complaint Center (IC3) reveal that phishing expeditions were the most highly reported crimes in the US in 2022, with 300,497 victims reported and over $52 million in losses.

The travel industry is no exception. The report by the Anti-Phishing Working Group (APWG) revealed that the travel industry was in the top 10 most targeted sectors. Forbes warns that as technology continues to integrate deeper into travel experiences, the risk of cyber-attacks while booking trips or accessing unsecured networks abroad is a growing concern.

So why is the travel industry a prime target? Online booking platforms handle vast amounts of sensitive data, from personal details to financial information — an attractive prize for cybercriminals. However, it's important to remember that phishing is a global issue impacting the entire online ecosystem — it does not reflect the security of our platform. We are committed to implementing advanced security measures to protect our users, which, combined with awareness, help to ensure the highest levels of protection.

2 How does phishing work?

Phishing is a form of cyber attack where fraudsters impersonate legitimate entities to trick you into revealing sensitive information. These attackers often use emails, messages, or fake websites that closely mimic authentic sources. Here's how phishing typically works:

Fake login pages:
Cybercriminals create counterfeit websites that look identical to the official login pages. A minor difference, such as an extra letter or slight URL alteration, can mislead even the most careful users.

Fraudulent offers:
Phishing emails or messages often contain urgent or enticing language, urging you to click on a link or provide your login credentials. They often use urgent offers like discounts, special deals, or limited-time promotions to push people into clicking links. Their goal is to capture your personal information before you realize what's happening.

Malicious ads:
When accessing a website, remember that not all ads are trustworthy sources. Before and after clicking on an ad, always double-check the URL to ensure you're on a legitimate site. Scammers often use misleading ads to direct users to fake pages that look real but are designed to steal your information.

Understanding and awareness of these tactics is the first step in protecting yourself and your business.

3 Steps to protect your account from phishing attacks

Implementing a few simple practices can go a long way in securing your accounts and preventing phishing attacks:

Check the URL carefully:
Always ensure you're on www.ratehawk.com. Fraudulent sites often have small variations in the URL (e.g., ratehwak.com instead of ratehawk.com).

Avoid clicking on suspicious links:
If you receive an unexpected email or message asking you to log in, do not click on the link. Instead, go directly to www.ratehawk.com/accounts/login.

Never share your login credentials:
RateHawk employees will never ask for your login or one-time password via email, phone, or social media. If you receive such a request, report it immediately.

Use strong and unique passwords:
Create a secure password using a mix of letters, numbers, and symbols. Avoid reusing passwords across different accounts. Passwords should be unique across different platforms. If one service is breached, using the same password everywhere could put your other accounts at serious risk.

Regularly update your password:
Changing your password every few months reduces the risk of unauthorized access.

By integrating these practices into your daily routine, you can build a robust defense against phishing attacks and keep your personal data protected. Empower yourself with these simple steps and be on the safe side with RateHawk!

Stay cyber safe with RateHawk

Supercharge your travel business with RateHawk!

We lead the way: 2.6M+ accommodation options worldwide from 300+ suppliers for air and train tickets, transfers, car rentals, and other travel services.

Get started for free

Contacts

ratehawk.com
support@ratehawk.com

Download

the RateHawk mobile app

Google Play

App Store