KnowBe4

Staying Safe From Summer Scammers 2024

As summer approaches, many people in the UK are excited about various events and travel plans. However, this excitement is also a prime opportunity for scammers to exploit. This report delves into the feedback from 2000 people in the UK on the prevalence of scams targeting individuals planning summer activities and provides advice on how to stay safe.

Statistics on Summer Plans

A significant portion of the UK (54%) has made summer plans, either planning to or having already booked tickets for various events and travels. The breakdown is as follows:

- **Travelling abroad:** 36%
- **Music festivals (e.g., Glastonbury, Reading/Leeds):** 15%
- **Euros Football Championships:** 13%
- **Wimbledon:** 11%
- **Olympics:** 10%
- **Taylor Swift's Eras Tour:** 9%

Impact of Scams

Among those who have been targeted by scams, 40% said they did report it to authorities, yet there have also been consequences:

Response to Data Breach Notifications

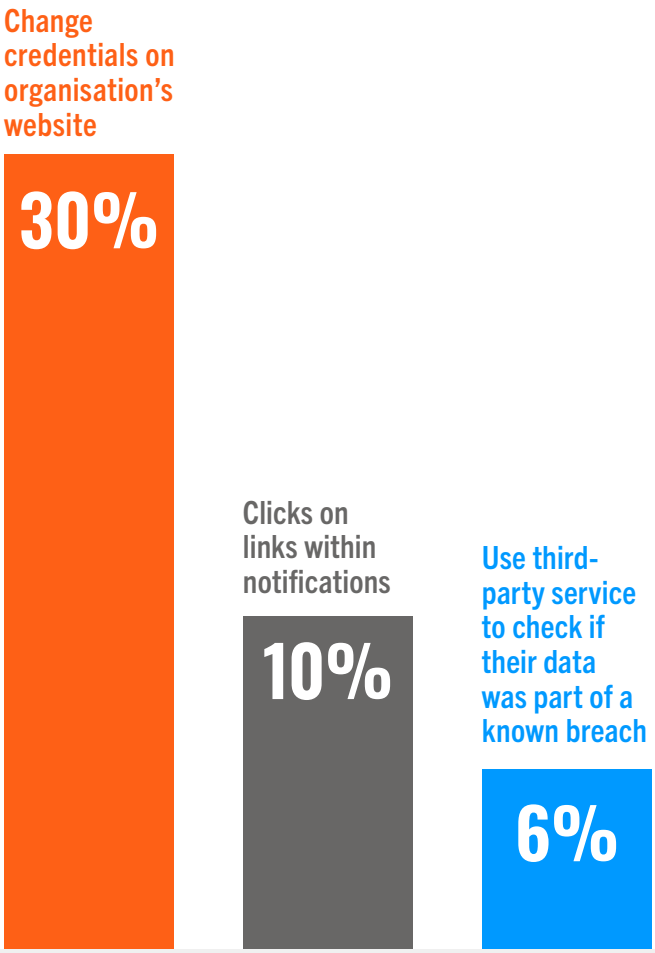
When it comes to responding to data breach notifications, actions vary:

Roughly a third (30%) would go directly to the organisation's website and change their credentials. This is the safest and most recommended course of action. By navigating directly to the official website, individuals can avoid phishing attempts that often use fraudulent links in emails or messages. This method ensures that users are interacting with the legitimate organisation, reducing the risk of further compromise.

One in ten would click on links within the notifications, despite this approach posing significant risks. Scammers frequently send phishing emails that mimic legitimate notifications, containing links that lead to malicious websites designed to steal credentials or install malware. Users who click on these links are at high risk of falling victim to additional scams.

Only 6% use a third-party service like haveibeenpwned. Utilising reputable third-party services to check if your information has been compromised is a prudent step. Services like haveibeenpwned provide valuable information on whether your data has been part of a known breach. However, this should be supplemented with actions such as changing passwords and enabling two-factor authentication on affected accounts.

Though a small amount (4%) would ignore the notification and carry on, ignoring a data breach notification is highly risky and can lead to severe consequences, such as unauthorised access to accounts, identity theft, and financial loss. Failure to take action leaves personal information vulnerable to misuse by malicious actors.



Attitudes Towards Data Security

25% **of people will provide their data** to a company or brand if they know it has **experienced a security breach or data leak.**

Despite the high risk of scams, there is a notable wariness about data security with only 25% of people likely to give their data to a company or brand if they know it has experienced a security breach or data leak. The statistic reflects an emotional response where consumers feel betrayed and are consequently hesitant to re-engage with the offending company.

Companies that experience data breaches face not only immediate technical and financial repercussions but also long-term reputational damage. The reluctance of 75% of individuals to provide their data post-breach highlights the critical need for businesses to prioritise data security to maintain customer trust and loyalty.

Tips for Staying Safe

Consumers looking to protect themselves from summer scams should consider the following tips:

Verify Sources: Always book tickets and make travel arrangements through official and reputable websites. Avoid clicking on links in unsolicited emails or messages.

Report Suspicious Activity: If a potential scam is encountered, report it to authorities. Prompt reporting can help prevent further victimisation and assist in tracking down scammers.

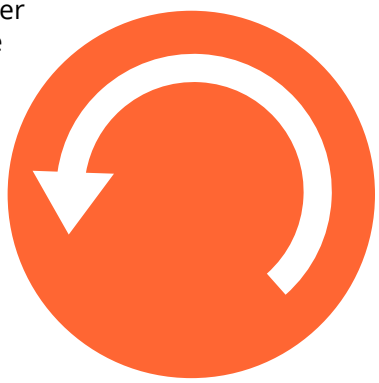
Protect Personal Information: Be cautious about sharing personal information online. Ensure websites are secure (look for "https" in the URL) before entering any data.

Monitor Accounts: Regularly check your bank and online accounts for any unusual activity. Set up alerts to be notified of any suspicious transactions.

Responding to Data Breaches: Change credentials directly on the official website rather than through links in emails. Use third-party services like haveibeenpwned to check if your information has been compromised. Finally, do not ignore data breach notifications; take immediate action to secure accounts.

Education: Stay informed about common scam tactics related to travel and events. Awareness is a critical step in prevention.

Conclusion



As the UK enjoys the summer and makes plans during the period, staying vigilant and informed can significantly reduce the risk of falling victim to scams.

By following the outlined tips and remaining cautious, consumers can protect themselves and their personal information from scammers who prey on the excitement of summer activities.