LPL Financial

Advertisement Fraud

Bad actors are constantly evolving their tactics to successfully commit fraud. As we continue to shop online, bad actors find more ways to target our commercial thoughts, creating a scam called Advertisement Fraud. Advertisement Fraud involves bad actors that impersonate reputable companies using fake search engine advertisements. The FBI has issued a warning about these scams due to their increased success in recent years.

How does this fraud work?

The goal of this fraud is to have the individual unknowingly expose sensitive information or to interact with malware via fake software. This starts with bad actors purchasing advertisements, to use later and appear in the internet top search results. When individuals do a search on the internet, they click the link to the fake advertisement in their search results and are taken to an imitation website. Once on the website two things occur:

1. The individual clicks on a link to download software that is malware.
2. The individual exposes their credentials.

Tips for staying safe

There are risks associated with everything we do, and unfortunately, this includes searching the internet. Some best practices for reducing your risks are included below:

- Be safe on the internet
  - Use internet browser address bar to search for the applicable company.
  - Imitation websites are created to mimic well-known companies, thoroughly review any website before entering any sensitive information.
  - Utilize an add blocker
- Think before you click
  - Never click a link or open an attachment from any unknown sources.
  - Hover mouse over URL to review webpage URL and confirm legitimacy
  - Avoid interacting with high pressure sales
- Protect your funds
  - Do not do business with anyone who asks for money in advance of awarding a prize.
  - Use a Credit Card to make payments, and do not give direct access to your bank account.

What should I do if I'm a victim of Advertisement Fraud?

1. **Stop all communication.** If you are in contact with a scammer, cease communication immediately.
2. **Report the incident.** You can file a complaint with the FTC on their website.
3. **Protect your identity.** Monitor your financial accounts, credit reports, and any other sensitive information for signs of unauthorized access and activity. With most accounts, you can place a fraud alert or a credit freeze to prevent further compromise.
4. **Document the incident.** Keep any record of communication and documentation related to the scam. This can be extremely useful when reporting the incident and resolving any issues with authorities.

Additional Considerations

If a scammer accessed your accounts…	Immediately change all passwords associated with the scam. Ensure the new password is strong and do not reuse passwords. Enable Multifactor Authentication (MFA) on all accounts.
If a scammer has access to financial information…	Contact your bank or credit card company immediately. They can help monitor your accounts for suspicious activity.
If a scammer has your social security number…	Place a fraud alert and initiate a credit freeze on your credit reports by contacting one of the three major credit bureaus. Additionally, file a report with the IRS and your bank so that they can protect your identity and monitor your accounts.