

SEO Scam Alert

What Every Client Needs to Know

By Matthew COSTIGAN, CFP®, CPA/PFS
Principal, Senior Financial Advisor for HBKS® Wealth Managers

and Scott VELMER
Manager, Vertilocity

IN TODAY'S DIGITAL WORLD, staying alert to online threats is more crucial than ever. Just like how technology is advancing, the tricks of online scammers are getting more cunning, too. Picture SEO scams as one of these crafty villains, specifically eyeing clients of financial institutions, and posing a real threat to their financial well-being.

Consider this interesting find from a 2023 Citi survey: While a solid 90 percent of U.S. adults were sure of their abilities to recognize and dodge financial scams, it turns out that 27 percent actually ended up being ensnared by one. This striking difference between confidence and experience highlights the need for a more robust approach — not just staying alert, but truly immersing ourselves in understanding these scams and developing the skills to deftly sidestep them.

UNDERSTANDING SEO SCAMS

Imagine you're navigating through a crowded market, looking for a genuine, high-quality watch. Amongst the genuine stalls, there's a stand selling what appears to be the same watch, but it's actually a clever imitation. That's the essence of SEO scams. They elevate fake websites to top search engine results, mimicking legitimate financial institutions so well that they fool even cautious individuals. When you click on these sites, it's like buying the imitation watch — it seems right until you realize it's not. These scams are a digital bait, set up to snatch your personal and financial information. They blend seamlessly into search results, making it a challenge to discern the real from the fake in the vast online marketplace.

Let's take a closer look at what happens once you land on one of these deceptive SEO scam sites. This is when the real trickery begins. Here's what happens next:



©mbbirdy and iStock

Remember that SEO constantly changes and no one can guarantee immediate results.



1. Fake error messages: You receive prompts asking you to contact a support number, which is operated by scammers.

2. Deceptive communication: You call them, worried about your account. The person on the other end — a scammer in disguise — spins a tale about a security breach. They're so convincing, you might even end up downloading software that gives them access to your device.

3. Compromised security: The endgame is here. They're after unauthorized access to your devices and personal info. It's a digital heist, hidden behind a facade of legitimacy.

RED FLAGS TO WATCH OUT FOR

Whether you're browsing online as a consumer or looking to enhance your business's online presence, recognizing these specific red flags can be your first line of defense against deceptive SEO practices.

For Consumers:

1. Unrealistic promises and guarantees: If a website guarantees instant top rankings or claims to have a secret formula for SEO success, be skeptical. SEO is a constantly changing field, and no one can guarantee immediate, top-tier results.

2. Misleading social media profiles and content: Be cautious of fake social media profiles or misleading blog posts and articles that use SEO tactics. They often contain false information or harmful links.

3. Overuse of keywords and hidden text: Websites that cram too many keywords or use hidden text are usually involved in unethical SEO practices. These tactics can negatively impact the user experience and are penalized by search engines.

4. Questionable reviews and testimonials: Be skeptical when reviews and testimonials on a website seem overly positive or fabricated. Additionally, a complete absence of testimonials can be just as telling. Authentic and genuine feedback is crucial for evaluating the credibility of any service or website.

For Businesses:

1. Suspicious directory listings and backlinks: Offers promising to enhance your search rankings through directories or backlinks should be approached with caution. Verify the effectiveness and legitimacy of these listings before investing.

2. Unsolicited SEO audit offers: If you receive an offer out of the blue for a free SEO audit, be wary. These are often used to sell unnecessary services or to exploit vulnerabilities in your website.

3. Guaranteed top rankings for keywords: Be wary of anyone who promises guaranteed rankings for specific keywords. SEO is an ongoing process and depends on many factors, including the ever-changing algorithms of search engines.

4. Fake reviews and testimonials for credibility: Alongside being cautious of overly positive reviews, also be aware of the absence of testimonials. A lack of genuine, verifiable feedback about an SEO service can be a significant red flag. It's important for businesses to verify that testimonials are from legitimate and reliable sources.



Today, it's just as crucial to protect your digital presence as it is to safeguard your physical wallet.

STEPS FOR PROTECTION

So, how do you keep safe from these digital wolves in sheep's clothing? To guard against these scams, here are some crucial steps I always recommend to my clients.

- **Get direct access:** Always go straight to the financial website by typing the address in your browser or using their official app. It's like knowing the exact location of the genuine watch stall in the market.
- **Use bookmarks:** Bookmark the real websites. This is like having a map to the right stall in your pocket.
- **Stay informed:** Keep up with the latest information on these scams. Knowledge is power! Here are a few good ways to stay informed:
 - Subscribe to security newsletters.
 - Attend webinars and workshops.
 - Follow trusted experts on social media.
 - Use online educational resources, like consumer.ftc.gov, to stay up to date.
 - Regularly consult with your financial advisor, like our team at HBKS. We're equipped with the latest resources and updates on current scamming trends. Plus, we can offer you tailored protective measures to keep your finances secure from these threats.
- **Report your suspicions:** Encounter something fishy? Make sure you report it ASAP to the right folks.

BRIDGING THE KNOWLEDGE GAP

In "Protect Yourself from Phishing Scams: How to Spot and Avoid Fraudsters Impersonating Financial Institutions," my colleagues Michael Wassmann and Scott Velmer explored various tactics to guard against online fraud. This advice is particularly relevant now as we address SEO scams. They emphasized the importance of recognizing phishing attempts, understanding the signs of fraudulent communication, and the necessity of maintaining robust security practices. Combining these insights with the specific strategies against SEO scams creates a comprehensive shield in the digital realm. It's about connecting the dots between different types of scams and reinforcing our defenses with a layered approach. Think of it as building a fortress where each brick represents a key piece of knowledge or a smart habit, making the entire structure — your digital safety — stronger and more resilient. "Like a fortress built brick by brick, your digital defenses require layers of knowledge and vigilance. Connect the dots between phishing and SEO scams to fortify your online presence." says Vertilocity's Scott Velmer.

In light of the persistent threat of financial fraud, it's crucial for us to maintain stringent security measures to safeguard our clients' interests. As such, we want to reiterate that we never accept trade instructions via voicemail or email. This precautionary measure aligns with the guidance provided by the Financial Industry Regulatory Authority (FINRA), who highlighted the risks associated with such practices in their 2012 notice.



In our interconnected world, it's just as crucial to protect your digital presence as it is to safeguard your physical wallet. By staying informed, smartly navigating the web, and adopting proactive measures, you can drastically lower the odds of falling prey to these sophisticated online scams. Stay alert, stay safe, and let's keep your digital journey secure and enjoyable. To further enhance our collective security, I encourage you to share this documentation with your network. By spreading awareness and knowledge, we can create a stronger, more resilient online community.

If you need further information or assistance in safeguarding your online presence against these scams, please don't hesitate to contact us. Our team is always ready to help you stay secure and informed.

IMPORTANT DISCLOSURES

The information included in this document is for general, informational purposes only. It does not contain any investment advice and does not address any individual facts and circumstances. As such, it cannot be relied on as providing any investment advice. If you would like investment advice regarding your specific facts and circumstances, please contact a qualified financial advisor.

Any investment involves some degree of risk, and different types of investments involve varying degrees of risk, including loss of principal. It should not be assumed that future performance of any specific investment, strategy or allocation (including those recommended by HBKS® Wealth Advisors) will be profitable or equal the corresponding indicated or intended results or performance level(s). Past performance of any security, indices, strategy or allocation may not be indicative of future results.

The historical and current information as to rules, laws, guidelines or benefits contained in this document is a summary of information obtained from or prepared by other sources. It has not been independently verified, but was obtained from sources believed to be reliable. HBKS® Wealth Advisors does not guarantee the accuracy of this information and does not assume liability for any errors in information obtained from or prepared by these other sources.

HBKS® Wealth Advisors is not a legal or accounting firm, and does not render legal, accounting or tax advice. You should contact an attorney or CPA if you wish to receive legal, accounting or tax advice.



Matthew Costigan, CFP, CPA/PFS

Principal, Senior Financial Advisor

Matthew Costigan is a principal and senior financial advisor in the HBKS® Pittsburgh office. His clients benefit from his extensive knowledge and practical experience with tax laws and best practices as they affect individuals, including planning for the tax impact of qualified and non-qualified investments.

Investment advisory services are offered through HBK Sorce Advisory LLC, doing business as HBKS Wealth Advisors. NOT FDIC INSURED - NOT BANK GUARANTEED - MAY LOSE VALUE, INCLUDING LOSS OF PRINCIPAL - NOT INSURED BY ANY STATE OR FEDERAL AGENCY