How to avoid falling victim to an online scam: Research says slow down

February 27 2023, by Yaniv Hanoch and Nicholas J. Kelley

Credit: AI-generated image (disclaimer)

Keeping up with the latest digital cons is exhausting. Fraudsters always seem to be one step ahead. But our study found there is one simple thing you can do to drastically reduce your chances of losing money to web scams: slow down.

In fact, among the various techniques used by scammers, creating a sense of urgency or the need to act or respond quickly is probably the most damaging. As with many legitimate sales, acting fast reduces your ability to think carefully, evaluate information and make a careful decision.

The COVID lockdowns made us all more reliant on online services such as shopping and banking. Quick to take advantage of this trend, scammers have since increased the rate and spectrum of online fraud. Cybersecurity company F5 found phishing attacks alone increased by over 200% during the height of the global pandemic, compared to the yearly average.

One fraud type many people fall victim to is fake websites (spoof legitimate business or government websites). According to a nonprofit that handles consumer complaints Better Business Bureau, fake websites are one of the leading reported scams. They caused estimated retail losses of approximately US$380 million (£316 million) in the US in 2022. Actually, losses are probably far higher because many cases go unreported.

We developed a series of experiments to evaluate what factors impact people's ability to distinguish between real and fake websites. In our studies, participants viewed screenshots of real and fake versions of six websites: Amazon, ASOS, Lloyds Bank, the World Health Organization COVID-19 donation website, PayPal and HMRC. The number of participants varied, but we had more than 200 in each experiment.

Each study involved asking participants whether they thought the screenshots showed authentic websites or not. Afterwards, they also took tests to evaluate their internet knowledge and analytical reasoning. Earlier research has shown analytical reasoning impacts our ability to tell between real and fake news and phishing emails.

People tend to employ two types of information processing—system one and system two. System one is quick, automatic, intuitive and related to our emotions. We know experts rely on system one to make quick decisions. System two is slow, conscious and laborious. The ability to perform well on analytical reasoning tasks has been associated with system two but not system one thinking. So we used analytical reasoning tasks as a proxy to help us tell whether people are leaning more on system one or two thinking.

An example of one of the questions in our analytical reasoning test is: "A bat and ball together cost $1.10. The bat costs $1.00 more than the ball. How much does the ball cost?"

Our results showed higher analytical reasoning ability was linked to a better ability to tell fake and real websites apart.

Other researchers have found time pressure reduces people's ability to detect phishing emails. It also tends to engage system one processing rather than system two. Scammers do not want us to carefully evaluate the information but engage emotionally with it. So our next step was to give people less time (about 10 seconds compared to 20 seconds in the first experiment) to do the task.

This time we used a new set of participants. We found participants who had less time to judge the credibility of a webpage showed poorer ability to discriminate between real and fake websites. They were about 50% less accurate compared to the group who had 20 seconds to decide whether a website was fake or real.

In our final study, we provided a new set of participants with 15 tips on how to spot fake websites (for instance, check the domain name). We also asked half of them to prioritize accuracy and take as much time as they needed while the other half were instructed to work as quickly as

possible. Working quickly rather than accurately was linked to worse performance, and to poor recall of the 15 tips we provided earlier.

With increasing internet use among all age groups, scammers are capitalizing on peoples' tendencies to use more intuitive information processing mechanisms to evaluate whether a website is legitimate. Scammers often design their solicitations in a way that encourages people to act quickly because they know that decisions made under such conditions are in their favor. For example, advertising that a discount is ending soon.

Much of the advice about how to identify fake websites suggests you carefully examine the domain name, check for the padlock symbol, use website checkers such as Get Safe Online, look for spelling errors, and be wary of deals that sound too good to be true. These suggestions, obviously, require time and deliberate action. Indeed, possibly the best advice you could follow is: slow down.

Provided by The Conversation