FACT CHECK

Fact check: Hackers using visually similar characters to deceive in phishing schemes

Rick Rouan USA TODAY

Published 5:06 p.m. ET Apr. 30, 2021 | Updated 5:07 p.m. ET Apr. 30, 2021

The claim: Hackers use visually similar characters to deceive people in online phishing schemes

Online attackers bent on stealing personal information are using a visual deception to trick people into visiting malicious websites, a post circulating on social media claims.

The April 20 Facebook post shows two web addresses that, at first glance, appear identical. A closer look, though, shows that one character – in this case, the letter "a" – is slightly different in each one.

"An average internet user can easily fall for this," the post reads. "Be careful for every mail requiring you to click on a link."

The post has been shared hundreds of times on Facebook.

The claim appears to be true. Credible sources dating back to the early 2000s give a similar warning against this kind of "spoof" of the website a user intends to visit. But similar exploitations have emerged recently as well.

The user who shared the post could not be reached for comment.

How does the attack work?

The attack is a form of "spoofing," when someone poses as a legitimate institution in an attempt to obtain personal information.

“Most people by now have gotten a little bit suspicious. … The idea is how can they trick you into thinking you know who it is or what it is when it isn’t,” said Stuart Madnick, founding director of Cybersecurity at MIT Sloan.

In this instance, it exploits the visual similarities between characters in the Roman alphabet used in the English language and the Cyrillic alphabet, which Britannica.com said was developed for Slavic-speaking people and is used in more than 50 languages, including Russian.

Substituting Cyrillic characters for Roman letters that look similar, such as the lowercase “a,” hackers can direct a user who intended to visit one website to another. Madnick said there are other ways to deceive without changing the alphabet, such as replacing a lowercase "L" with a capital "I" in some fonts.

“Instead of going to a legitimate site, you may be directed to a malicious site, which could look identical to the real one,” notes a 2008 security notice from the U.S. Cybersecurity & Infrastructure Security Agency. “If you submit personal or financial information while on the malicious site, the attacker could collect the information and then use and/or sell it."

Fact check: Coronavirus vaccines don’t cause death, won’t decimate world’s population

The scheme is possible because of internationalized domain names and how web browsers read them, according to the agency’s notice, which was updated in 2019.

The so-called “homograph” attacks have been around since the early 2000s. A 2005 post on The Register, an online technology news publication, called them “a new vector for phishing attacks.”

But they have popped up again recently. Last year, researchers discovered domain names designed to deceive users into thinking they were going to a legitimate website, The Register reported, despite efforts to contain the problem.

“These bogus sites are designed to look real while phishing (to gather) credentials or distributing malware,” according to the March 2020 post. “You think you’re logging into Google.com from an email or instant-chat link, but really you’re handing over your password to a crook.”

CISA also warned of the potential for homograph attacks in a December 2020 alert about cyber attacks designed to disrupt remote learning as children attended virtual classrooms during the COVID-19 pandemic.

How do you avoid falling into the trap?

Spoofed hyperlinks and websites are a red flag for a potential attempt to steal personal information, according to CISA, part of the U.S. Department of Homeland Security. CISA recommends three steps to avoid falling victim to the scheme:

- Avoid clicking on links and instead type the web address into an internet browser.
- Keep web browsers up to date because older versions have fewer protections in place.
- Hover over links before clicking on them to see the true destination. If the web address the link directs to is unfamiliar, it might be an attempt to deceive you.

People should assume they eventually will be the target of an attack and take steps in advance to mitigate any damage, MIT's Madnick said. He recommended using software to protect against viruses and malware and having data backups that would make ransomware attacks less effective.

Our ruling: True

The claim that hackers use letters that look similar but come from another alphabet to deceive people in online phishing schemes is TRUE, based on our research. The deception known as a homograph attack has been going on since at least the early 2000s. Letters from the Cyrillic alphabet are substituted for those that are visually similar in the Latin alphabet to direct unknowing users to malicious websites.

Our fact-check sources:

- MIT Sloan, accessed April 30, Bio for Stuart Madnick
- Britannica.com, accessed April 30, Cyrillic alphabet entry
- U.S. Cybersecurity and Infrastructure Security Agency, Aug. 6, 2008, Understanding Internationalized Domain Names
- The Register, Feb. 10, 2005, Beware the unexpected attack vector
- The Register, March 4, 2020, It has been 15 years, and we're still reporting homograph attacks – web domains that stealthily use non-Latin characters to appear legit
- U.S. Cybersecurity and Infrastructure Security Agency, Dec. 10, 2020, Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data
- U.S. Cybersecurity and Infrastructure Security Agency, Oct. 22, 2009, Avoiding Social Engineering and Phishing Attacks

- Mashable, March 6, 2020, Major domain name bug allowed hackers to register malicious domains
- Bleepingcomputer.com, March 4, 2020, Zero-Day Bug Allowed Attackers to Register Malicious Domains

Thank you for supporting our journalism. You can subscribe to our print edition, ad-free app or electronic newspaper replica here.

Our fact check work is supported in part by a grant from Facebook.