



Video transcript: "Protecting Your Accounts From Scams | Treasury Management | Regions Bank"

Video source: [[https://youtu.be/mb8\\_yZvpO0w](https://youtu.be/mb8_yZvpO0w) ]

[The Regions logo appears. The words "Website Spoofing & Fraud Prevention," appear. The green triangle of the Regions logo turns and morphs into a play button icon. The user clicks the play button. Ominous music begins playing.]

**VOICE-OVER:** Fraudulent online activity is on the rise! Phony or spoofed websites can look nearly identical to bank login pages, including Regions OnePass.

[Numbers begin moving rapidly on screen with the words, "Fraudulent online activity is on the rise!" appearing within the numbers. A search engine on computer browser appears with "Regions OnePass" in the search bar. The screen zooms in to show search results that are not legitimate.]

**VOICE-OVER:** These fake websites could be accidentally accessed simply by searching specific key words. The only way to safely log in to Regions OnePass is to type in the URL [onepass.regions.com/login](http://onepass.regions.com/login).

[A man with a dark hat, glasses and black gloves appears above the search page and is holding the screen. The screen scrolls up and the words, "Regions OnePass" are typed into the search bar. The screen shifts right, and the URL [onepass.regions.com/login](http://onepass.regions.com/login) is typed into the bar at the top of the screen. A big green circle is in the background with a checkmark and lock icons floating around it.]

**VOICE-OVER:** Here's what happens: You search Regions OnePass, iTreasury, or something similar within your online browser. A list of ads and pages comes up and they all look legitimate.

[The words, "Here's what happens:" appear on screen. The top of the search screen is showing with the words, "Regions OnePass" and then "Regions iTreasury" typed in the search bar. The page opens up wider to show the search results.

**VOICE-OVER:** However, if you look closely at the URL or web address, most of them are NOT affiliated with Regions bank at all!

[A closer view of the URL shows <http://www.regions-1pass.online> is not a valid URL

and is not associated with Regions at all. Another URL is shown <https://www.regions-one.net> and it's not legitimate either. Both are spoofed or phony websites that could appear when searching online.]

**VOICE-OVER:** If you happen to click on the fraudulent website and then provide your username and password on the login screen, the fraudsters can take the information and may gain full access to your accounts.

[The user hovers over the top phony web address and clicks on it. What looks like the Regions OnePass login page shows up. The user types in their Login ID and Password. The mysterious looking man shows up at the top of the screen grabbing the search bar. Two icons with white exclamation points within orange triangles show up around the phony Regions OnePass® Login page. The page turns into an account information page and the Current Available balance is highlighted with another warning icon.]

**VOICE-OVER:** It's important to remember, **search engines should never be used for navigating to a login page**, as it could lead to a phony website.

[The screen shifts to the right, and the search engine page comes back up with the mysterious man holding the page. The words, "Regions OnePass" and "Regions iTreasury" are both typed into the search bar. The screen zooms out and shows the incorrect login pages for OnePass. The two incorrect URLs are highlighted again with error icons.]

**VOICE-OVER:** Establish safe online practices by entering the specific web address or URL provided by your bank directly into the address bar of your browser. The URL for signing into Regions OnePass for Treasury Management services is [onepass.regions.com/login](https://onepass.regions.com/login).

[A woman appears to be looking at a computer. The screen zooms into her browser to see the correct URL being typed into the top of the screen, [onepass.regions.com/login](https://onepass.regions.com/login). The screen zooms out to show the full and correct URL.]

**VOICE-OVER:** Be sure to bookmark the OnePass URL for ease of use in the future or create a shortcut. Always be on the lookout for poor spelling, transposed characters and/or design issues indicating a spoofed website.

[The user then goes to the side of the page and bookmarks the URL for future use. Another woman appears to be sitting at a desk with a computer in front of her. The



words, “regions onepas login,” and “Enter yuor login ID.” appear to showcase poor spelling of spoofed or fraudulent websites. One login screen is shown on the left and is fake and the Regions OnePass® Login page on the right is the correct one to use. The incorrect design issues show the user which one is legitimate.]

**VOICE-OVER:** If you feel you are a victim of fraud, file a report with IC3.gov and contact your local office of the FBI.

[The words, “If you feel you are a victim of fraud, file a report with IC3.gov and contact your local office of the FBI,” appear on screen.]

**VOICE-OVER:** Learn more about fraud prevention at [regions.com/stopfraud](https://regions.com/stopfraud) or [regions.com/fraudprevention](https://regions.com/fraudprevention).

[The words, “Learn more about fraud prevention at [regions.com/stopfraud](https://regions.com/stopfraud) or [regions.com/fraudprevention](https://regions.com/fraudprevention),” appear on screen. The Regions logo appears again, and the music fades down.]

[The following disclosures display onscreen. The information presented is general in nature and should not be considered, legal, accounting or tax advice. Regions reminds its customers that they should be vigilant about fraud and security and that they are responsible for taking action to protect their computer systems. Fraud prevention requires a continuous review of your policies and practices, as the threat evolves daily. There is no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur.

Visit [regions.com/stopfraud](https://regions.com/stopfraud), or speak with your Treasury Management Officer for further information on how you can help prevent fraud.

© 2025 All Rights Reserved, Regions Bank, Member FDIC. Equal Housing Lender. Only bank deposit products are FDIC insured. Regions, the Regions logo and the LifeGreen bike are registered trademarks of Regions Bank. The LifeGreen color is a trademark of Regions Bank.]