

Recipient: David Kaneshiro, Chief Technology Officer, World Vision

For: All Employees

Copy Date: Published on Corporate Intranet April 05, 2018

Headline: Action needed: The time to protect WVUS from high-risk data is now!

Imagine your doctor told you about an illness in the United States that is going to make half of the population sick. You would want to protect yourself against that disease. Last summer, such an occurrence did happen, but your health was not affected. Instead, personal data was the target. Equifax, one of the largest possessors of personal information was the victim of the worst data breach in U.S. history. Social security numbers, birthdays, and addresses of more than 143 million Americans were exposed. ⁽¹⁾

Now, imagine that your doctor provided you with proper medicine, but it sat on the counter without being taken, and you became sick. In the same way, Equifax did not apply a security patch in a timely fashion which would have prevented the breach.

Without the help of every employee, our data remains at risk.

Your ISG department has been implementing a new security application called "Zscaler." This application guards our internet traffic and intercepts high-risk data before it can harm or disable our systems. However, even the most rigorous defense is ineffective if we ignore or disregard it.

Just as we strive to be good stewards of our time and money, here at World Vision, the ISG department asks you to be good stewards of our data as well by following these three simple steps.

Step 1: Install Zscaler and Reboot Your Computers

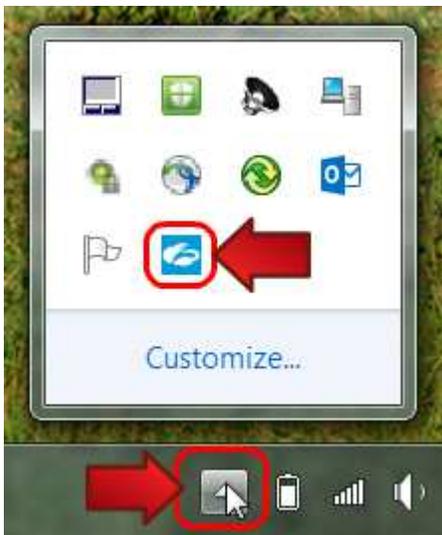
The most important action you can take to secure our data is to heed the installation alert on your computer, including any spares you may have stored away. Then, decide on a convenient time of day and reboot your computer. Perhaps you can arrive ten minutes early or step away from your desk for lunch. You can decide on a time which will have the least impact on your daily tasks while your computer restarts. Rebooting your computer is the only way to ensure that the installation process completes.

Step 2: Login to Zscaler.

Zscaler requires that you log in but, just like logging in to your computer first thing in the morning, logging into Zscaler is easy. Use the same username and password for your computer, and complete the simple task in seconds.

Step 3: Confirm Zscaler is Enabled.

- A quick check of your taskbar will show you right away if Zscaler is running correctly.
Click on the arrow in the lower right-hand corner of your screen to see which programs are running on your computer.
- Locate the Zscaler icon (fig 1).
If the icon is blue, congratulations, you have successfully secured your computer. (For extra confirmation, place your mouse over the icon, and you should see "Service Enabled" appear.)
- If you do not see the Zscaler icon or you see the icon but it is grey, please contact the Help Desk right away at 5100 for friendly assistance.



(fig 1)

An attack on our computers is a real threat, but by being diligent and following the three simple steps above, you can help us take steps to ensure safe and secure data.

⁽¹⁾ <https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686>