# Table of Contents

Table of Contents ............................................ 1
PC support ....................................................... 2
  Disable Pop-up Blockers .................................. 3
  Endpoint protection FAQ ................................... 11
PC support
Disable Pop-up Blockers

How to Disable Pop-Up Blockers

Click [here](#) for a step-by-step guide on how to disable the pop-up blocker on Google Chrome.

Click [here](#) for a step-by-step guide on how to disable the pop-up blocker on Mozilla Firefox.

Click [here](#) for a step-by-step guide on how to disable the pop-up blocker on Microsoft Edge.

Click [here](#) for a step-by-step guide on how to disable the pop-up blocker on Safari.

**Google Chrome**

1. Click on the **three dots** in the upper right hand corner of the screen.

![Google Chrome settings](#)

2. Click on **Settings** in the drop down menu.

![Google Chrome settings](#)

3. In this new window, you should see a **Search settings** box at the top. Type in "pop-ups"

![Google Chrome settings](#)

4. Once you're done typing **pop-ups**, you should see an option called **Site Settings**. The term **pop-ups** will be highlighted under **Site Settings**, which means it is located under this category. Click on **Site Settings**.

![Google Chrome settings](#)
5. Scroll down to find **Pop-ups and redirects** and click on it.

6. With the option "Blocked (recommended)", if your slider is grey then it indicates that pop-ups are currently being **blocked**. Click on the slider to move it to the other side.
7. Once you have clicked on the slider it should now be blue. The Blocked(recommended) changes to say Allowed instead which means that pop-ups are being allowed to appear.

Mozilla Firefox

1. Click on the three horizontal lines in the upper right hand corner of your screen.

2. Click on Options.

3. You should now see this window and also see the Find in Options box. Start to type pop-up.
4. Once you are done typing **pop-up** you should see the **Block pop-up windows** checkbox.

5. Click on the checkbox so it matches the image below.
1. Click on the **three dots** located in the upper right hand corner of your screen.

2. Click on **Settings**.

3. You should see this screen now and the **Search settings** box begin to type **pop-up**.

4. Once done typing **pop-up**, you should see the **Pop-ups and redirects setting** being highlighted. Here you can see underneath the settings if pop-ups are being **allowed** or **blocked**. In this case, it is already **allowed**. If it is **blocked** proceed to the next step.
5. If it is blocked you should then see the slider on the left and it being blue like the image below. Click on the slider so that it turns grey.

6. After clicking the slider you should see the slider on the left this indicates that pop-ups are being allowed now.
1. Click "Safari" in the upper left corner of the screen and select "Preferences"

2. This window will appear. Click "Security" from the list of categories

3. Uncheck the box next to "Block pop-up windows." This will disable the setting that blocks pop-up windows from appearing.
Congratulations! You've successfully disabled the pop-up blockers feature in your respective browser type.
Online security threats from scams to ransomware continue to increase. As employees of a public institution whose salary information is publicly available, who have access to costly resources that others want to gain access to, and who may also be handling sensitive data, our computers and online activities have the potential to be a portal to reams of information, and breaches can lead to catastrophic professional and personal results.

To prevent such problems and to ensure only authorized access to information, URI will be implementing a new endpoint protection policy. This policy is intended to protect both the individual intellectual property of the faculty as well as the confidentiality of URI-held data such as your social security number, health data, student grades, and similar items.

What kinds of things can I access without a VPN?
As we move to implement these policies, many of the common-use application suites will remain accessible without the use of the VPN. Among these are the Google suite of applications, Microsoft Office, Brightspace and similar systems. However, the use of the VPN for these purposes is highly recommended, as this both encrypts your data traffic to these systems and offers two-factor authentication to help ensure identity verification.

What resources would I need to use a VPN for?
Any time you are accessing sensitive University data, such as the HR or Financials system of the University.

What constitutes sensitive data and who defines it?
The data governance subgroup of the larger IT Governance committee is responsible for data classification. The group is just now resuming work after the pandemic and will be working on this and other data governance issues. In the meantime, please use your best judgment on this - one reasonable metric might be: if this information I am working with should become public on the internet, will it potentially harm anyone?

How do I comply?
The best source of assistance is your College or Departmental IT support person. For those without such support staff available, please contact the IT Service Desk as soon as possible - we also have limited desktop support staff, and depending on volume it may take some time to get you the assistance you need.

What about my personal phone - what do I need to do?
Depending on the type of device, it may fall into either the phone or desktop support category. Most Windows-based devices will support the current VPN, authentication, and endpoint protection software. Apple devices will most likely support the same systems as the phones.

I was never issued a University laptop or computer. What should I do?
Please speak with your department head. The Faculty Senate Committee on IT and Infrastructure is finalizing their report on equitable access to computing resources which will also be used as input to estimate the financial impact and begin prioritizing these needs.

What about my graduate students who are using their own devices?
Graduate students accessing sensitive or restricted data systems at URI also need to be in compliance with the endpoint protection policy. Your local IT resource or the ITS Service Desk can assist them as well.

Will there be exceptions?
Yes. ITS is going to be working with a group of faculty from Engineering, where many research projects need direct, low-level access to the equipment to help us figure out the exception process to ensure continued research productivity. Once this work is completed, the policy website will also have an accompanying process document.