Cybersecurity: https://cybersecurity.osu.edu/cybersecurity-you

Cybercrime is continually on the rise, but you can take steps to protect yourself. Enterprise Security works to ensure the security of Ohio State systems and data, but we want to help you keep your information and devices secure even when you're not at school or work. However you use technology in your daily life -- whether you are a minimalist or a prolific techie -- our site will give you the information you need to keep your devices and information secure.

Enterprise Security keeps Ohio State's users and data secure Enterprise Security works to ensure that users adapt safe practices when they use technology to keep their information safe as well as securing the data entrusted to The Ohio State University. Not only do external regulators require that our health, financial, student and research data be securely managed, but we also need to provide the high level of data security expected by our students and partners. Translating Enterprise Security strategy into execution is the work of all Buckeyes, requiring an unwavering commitment to our stakeholders and ongoing collaboration across the university community.

- **Report an Incident, Phishing or Spam:** https://cybersecurity.osu.edu/about

Responsible Use of University Computing and Network Resources Policy

https://it.osu.edu/sites/default/files/files-1477502439/responsible-use-of-university-computing-and-network-resources-policy.pdf

- **FAQs:** https://it.osu.edu/policies-and-standards/policy-faqs

Institutional Data Policy https://ocio.osu.edu/policy/policies/idp

Steps to connect to the Ohio State University School of Earth Sciences VPN:
https://osuasc.teamdynamix.com/TDClient/KB/ArticleDet?ID=14542

What Type of Data am I Working With?

- **IDP (Institutional Data Policy) Calculator**

  https://cybersecurity.osu.edu/idp-calculator

The newly released IDP Calculator Page is a job aid, designed to compile the information from the IDP supporting documents listed below:

- Institutional Data Element Classification Assignments(link is external)
- Permitted Data Usage By Activity(link is external)
- Permitted Data Usage By Service(link is external)

Using this Calculator, you simply select the data elements which are in your data source and click "Submit" at the bottom. The resulting page will inform you what services and activities are permitted as well as elements which are controlled by regulations. At the bottom of this resulting page will list the Data levels of each element that you know as well as the overall classification of your data source. This will help you to know what data element is causing the overall classification. Any elements not in the below list should be considered S2.

OSU Data Classification Assignments

From the Office of the Chief Information Officer, Institutional Data Element Classification Assignments

https://cybersecurity.osu.edu/system/files/osuidp-dataelementclassificationassignments.pdf

University Mail Encryption

From the IT Service Desk
https://osuitsm.service-now.com/selfservice/kb_view.do?sys_kb_id=821fad9408100504cb5eb1c5f01fe40a&sysparm_language=&sysparm_nameofstack=&sysparm_search=

VPN Services (Virtual Private Network)
https://cybersecurity.osu.edu/cybersecurity-you/use-right-tools/vpn-services

Steps to connect to the Ohio State University School of Earth Sciences VPN:
https://osuasc.teamdynamix.com/TDClient/KB/ArticleDet?ID=14542

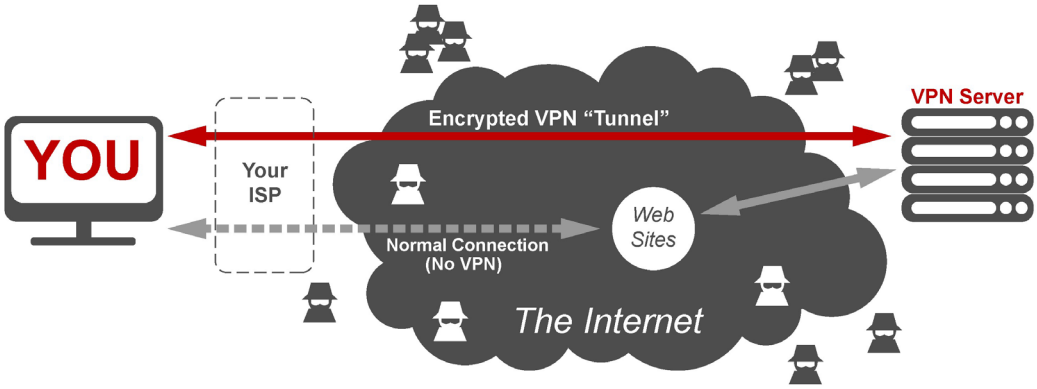
Here's the deal. I'm gonna give it to you straight, you ready? Your internet traffic is not always private. Eavesdroppers can see what websites you're visiting and they can sometimes monitor other sensitive information that you send through the internet. But there is a way to make your connection way more private and secure! It's called a Virtual Private Network (VPN). Let's break it down.

First, let's start by talking about what exactly isn't private and who might be monitoring your internet traffic. You might think it's just bad guys but actually there are a lot of "good guys" that spy on your traffic too. You probably even gave them permission! For example, the company you pay to provide you with internet service (your internet service provider or ISP) almost certainly monitors your internet traffic and sells information about you to marketing companies. That's why those rainbow striped toesy socks you almost bought keep showing up in internet advertisements! ISPs can also determine when you're watching a streaming service like Netflix and they can even tell what movie you're watching!! If that doesn't seem like a big deal to you, consider that most internet service providers also sell cable service… and it is theoretically possible that your ISP might slow down your streaming services so that you might get frustrated and decide to "un-cut" that cable service you got rid of last year. Not all ISPs do this. Some believe in "Net Neutrality," which means that they will not ever slow down your traffic for any reason. But they will still monitor you!

Ok, so what if you're not too concerned about privacy issues or net neutrality? You should know that there are other situations where internet hooligans can watch your internet traffic in an attempt to steal your identity, your payment information or other sensitive information. Public Wi-Fi hotspots are perfect locations for someone to do that, because these locations are almost always unsecure. For example, when you connect to public internet at an airport or a coffee shop, anyone else that is sitting nearby can just watch all of your internet traffic. If you're sending unsecured emails, connecting to unsecured websites or sending and receiving important files, these eavesdroppers can collect whatever it is you're sending. That's because your account credentials, payment information, intellectual property related to your work or other sensitive data could be of value on the dark web.

So what's this VPN thing and how does it help?

Okay, okay, slow down, we'll get to that. First, let us say that in an ideal world you'd have a truly private physical wire connecting your computer to any other machine or website with which you need to communicate. With a dedicated physical line, it would be really hard for anyone to watch your traffic because they'd have to tap into the line. But having all those wires would be really impractical, right?! No one could afford the cost of setting that up. Plus, there would be way too many wires everywhere! No one likes wires anyway, that's why we invented wireless!!



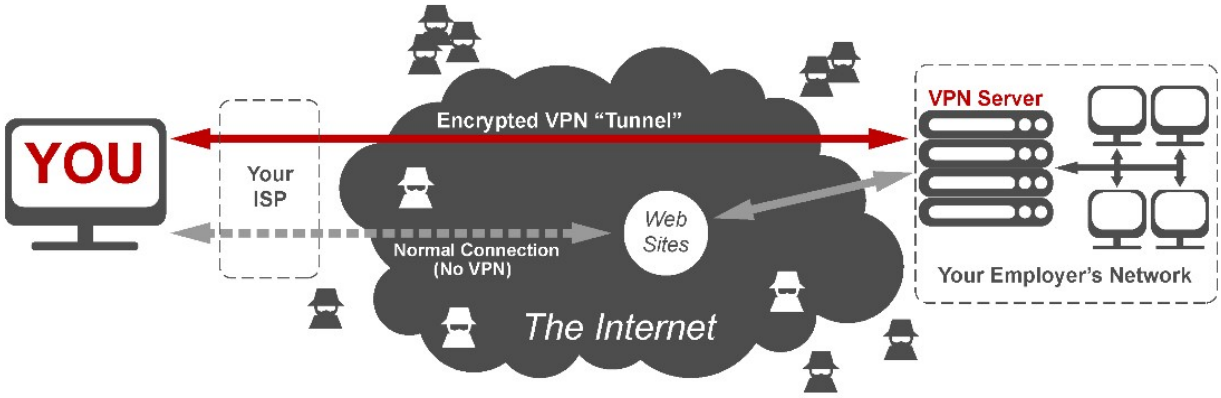
A Virtual Private Network provides a practical alternative. A VPN is exactly what it sounds like; a private communication channel that is established "virtually" over a non-private physical network like the internet. To understand how this works, take a look at the image below and then we'll break it down.

When you set up a VPN, what you are doing is establishing an encrypted connection between your computer and a "VPN server" somewhere. Sometimes we call this a VPN "Tunnel" because, metaphorically, it's kind of like a really secure, physical tunnel through which your data will be sent. In reality the data is being encrypted. This encryption is strong enough that eavesdroppers cannot see what's in the data at all. In fact, no one between you and the VPN server can see the data, including your ISP!

So what happens to the data when it gets to the VPN server? Good question! The VPN server is really just a middleman. If you are trying to reach a website while connected to a VPN, you send your encrypted traffic to the VPN server and then it forwards that traffic on to the website as if the traffic originated from the VPN server. That's right, the VPN masks the origin of the data so really no one could ever tell that it came from anywhere but the VPN. It's like when Bruce Wayne goes down to the basement of Wayne Manor, gets all dressed up, drives the Batmobile down some long underground tunnel and then pop's out of a waterfall somewhere. Even if there was someone at the waterfall, they aren't gonna associate the Batmobile with Bruce Wayne, because… why would they?

VPNs can also allow you to safely connect to a remote network of computers as if you are there. In that case, the VPN server is actually physically connected to a network of machines. The server can still forward your traffic on to the internet but it can also forward it to another machine in the network to which it is connected. This kind of VPN is used commonly by businesses to allow their employees to remotely connect to their protected internal networks. Take a look at the figure below.

VPNs at Ohio State



Ohio State has a VPN service that will protect your internet traffic and allow you to connect to the network as if you are on campus. If you are a university employee you can open your "Cisco AnyConnect Secure Mobility Client" on your university-managed device and connect to the network at Ohio State from anywhere in the world. This can allow you to safely access files that you would normally only be able to see if you connect from a location on campus.

VPNs for personal Use

You can, and should, use a VPN in your personal life too. There are VPN services you can pay for that have servers all over the world. Once you sign up it will actually let you decide which server you want to route your traffic through. After that, when you connect to the VPN, your traffic will appear to originate from that same server no matter where you are in the world. It's your "Batcave waterfall!" Just like with the Ohio State VPN, you should connect your personal devices to your VPN service when accessing the internet from public places or networks you don't trust.

Some drawbacks of VPNs

While VPNs stop cyber-hoodlums and your ISP from seeing your internet traffic, they will also prevent firewalls from inspecting that traffic, which will defeat the firewall as a protective measure. This is why it's important to have a firewall set up on your computer and not just rely on network-based firewalls. Your VPN server will also have a firewall on their end, but this is an important detail to keep in mind if you are ever setting up a network. When selecting a VPN service for personal use, you should also keep in mind that the VPN service can actually spy on your traffic just like your ISP can. Some of these services swear that they don't monitor your traffic and they really don't have a vested interest in slowing your traffic down so VPNs can definitely be an improvement over ISPs in terms of privacy and net neutrality. Just make sure you read their monitoring policy carefully.

Steps to connect to the Ohio State University School of Earth Sciences VPN:

https://osuasc.teamdynamix.com/TDClient/KB/ArticleDet?ID=14542

Export Control, International Travel and Data Security

http://orc.osu.edu/regulations-policies/exportcontrol/

What is Export Control?

The U.S. government regulates the transfer of information, commodities, technology, and software considered to be strategically important to the U.S. in the interest of national security, economic and/or foreign policy concerns. There is a complicated network of federal agencies and inter-related regulations that govern exports collectively referred to as "Export Controls." In brief, Export Controls regulate the shipment or transfer, by whatever means, of controlled items, software, technology, or services out of U.S. (termed an "Export"). Perhaps of even more consequence to the university, is that the government also restricts the release of certain information to foreign nationals here in the U.S. (referred to as a "Deemed Export"). Export Controls have the potential to severely limit the research opportunities of university faculty and their students and staff, as well as to prevent international collaboration in certain research areas. Non-compliance with export controls can result in severe monetary and criminal penalties against both an individual as well as the university, and can result in the loss of research contracts, governmental funding, and the ability to export items.

What do OSU personnel need to do?

In order to ensure compliance with export controls, it is critically important for university personnel to identify when their activities may trigger export controls. When export controls apply, individuals must take the appropriate steps to obtain any required governmental licenses, monitor and control access to restricted information, and safeguard all controlled materials.

What kinds of activities might trigger export control issues?

Research in export restricted science and engineering areas – examples include:

- Military or Defense Articles and Services
- High Performance Computing
- Dual Use Technologies (technologies with both a military and commercial application)
- Encryption Technology
- Missiles & Missile Technology
- Chemical/Biological Weapons
- Nuclear Technology
- Select Agents & Toxins (see Select Agent/Toxin list)
- Space Technology & Satellites
- Medical Lasers

Traveling overseas with high tech equipment, confidential, unpublished, or proprietary information or data – Traveling with certain types of high tech equipment including but not limited to advanced GPS units, scientific equipment, or with controlled, proprietary or unpublished data in any format may require an export license depending on your travel destination. See International Travel for more information.

Traveling with laptop computers, web-enabled cell phones and other personal equipment – Laptop computers, web-enabled cell phones, and other electronics containing encryption hardware or software and/or proprietary software can require an export license to certain destinations. In general, an export license will be required to take any items to or through any U.S. sanctioned country (e.g., Iran, Syria, Cuba, Sudan, and North Korea).

Use of 3rd Party Export Controlled Technology or Information – University activities involving the use of export controlled information, items, or technology received from outside the university are not protected under the Fundamental Research Exclusion and all research involving the use of export restricted technology is subject to all export controls. For help in determining export control issues see Incoming Export Control Information Questionnaire.

Sponsored research containing contractual restrictions on publication or dissemination – The vast majority of research done at the university is shielded from export controls under the Fundamental Research Exclusion. However, this protection is lost whenever the university or the researcher agrees to allow any restrictions on the publication, dissemination, or access to the research by foreign nationals.

Shipping or Taking Items Overseas – University activities that involve the transfer of project information, equipment, materials, or technology out of the U.S. by whatever means will be subject to export controls and may require export license(s) depending on the item, destination, recipient, and end-use.

Providing Financial Support/International Financial Transactions – University activities that involve the international payment of funds to non-U.S. persons abroad need to be verified to ensure that the university is not inadvertently providing financial assistance to a blocked or sanctioned entity. Examples include providing support via a subcontract to a non-U.S. university or providing payments to research subjects in other countries. Contact exportcontrol@osu.edu if your activity involves payment to persons or organizations outside the U.S.

International Collaborations & Presentations – University activities that involve foreign national faculty, students, staff, visiting foreign scientists or collaborator(s), or other foreign entities (e.g., non-U.S. company, university or other organization) or research that will include travel to international conferences to present unpublished results may be subject to export controls especially if any of the foreign nationals are from embargoed or sanctioned countries. See International Collaborations for more information.

International Field Work – Research projects where any part of the research will take place outside the U.S. (e.g., field work outside the U.S.) may not qualify under the Fundamental Research Exclusion and may be subject to export controls. For help in determining potential export control issues see the International Research Export Control Questionnaire.

International Consulting – Providing professional consulting services overseas, especially to embargoed or sanctioned countries (e.g., Iran, Syria, Cuba, Sudan and North Korea) is, in most cases, strictly prohibited.

Where can you get help?

SES Data Security and Computer Contacts

- **Brent Curtiss.3**
  Email for IT customer service asctech@osu.edu
  125 South Oval Mall Rm 200F
  (614) 688-3758
  Data security, computers, computer related issues

- **Theresa Mooney.175**
  125 South Oval Mall Rm 275E
  (614)292-6628
  Portable electronics, off campus equipment and international travel

- **Soyoung Carpenter.634**
  125 South Oval Mall Rm 275N
  (614) 688-2884
  SES Manager, back up