ORU IT 2018-19

Oral Roberts University Information Technology Student Guide

August 2018

Contents

Contacting ORU IT

There are several ways to contact ORU IT for either technical help and/or information:

- Phone: 918-495-6321
- Email: studenthelpdesk@oru.edu
- Twitter: @ORU_IT
- In Person: IT Concierge Desk LRC3 (outside the Hava Java) or IT Offices Located on GC 4.5 East
- Website: http://it.oru.edu

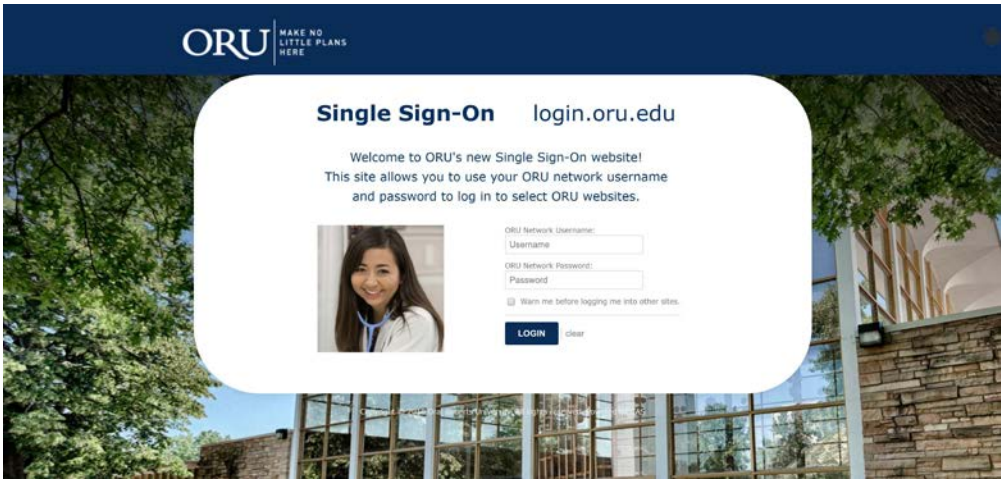
Accessing ORU-Student Wireless on Campus

1. Go to your wireless connection icon (generally found on your taskbar in both the Windows and Mac OS or in the settings menu on your mobile devices).
2. Turn on your wireless.
3. Locate the ORU-Student network.

How to Log into the ORU Web Apps

New Website for Single Sign-on

https://login.oru.edu is ORU's new Single Sign-On web site. The site allows you to use your single ORU network username and password.



Vision

There are two ways to log into http://vision.oru.edu

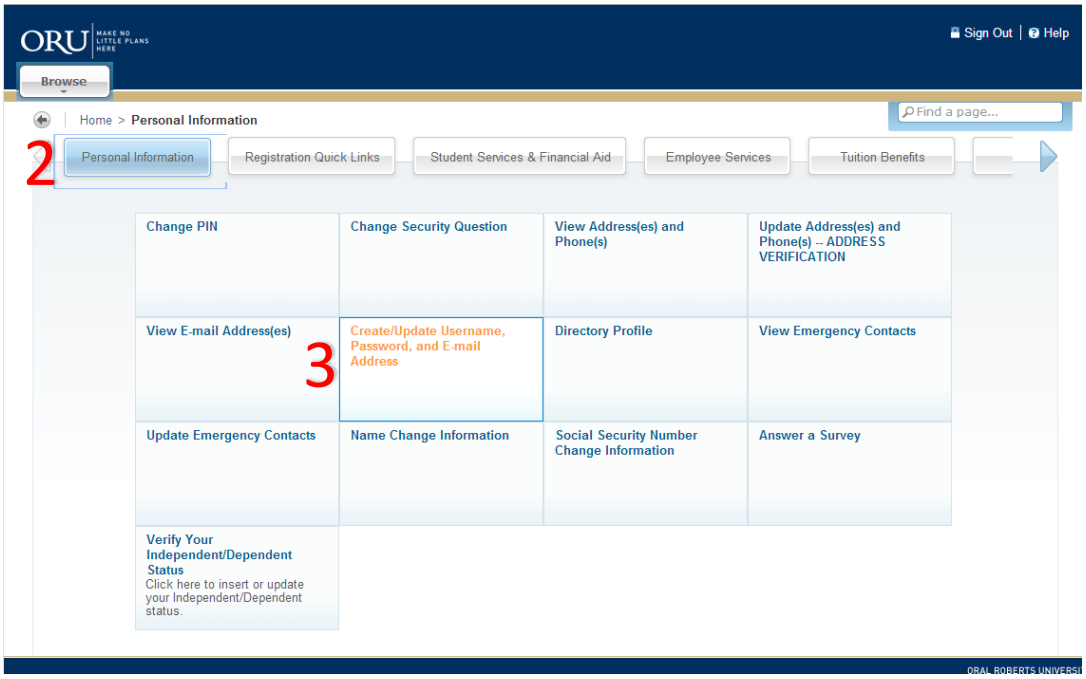
- using your network username and password
- **OR** using your Z number and PIN

Office 365 (Student Email)

- You will use your **network username@oru.edu** and **password** to log into http://mail.oru.edu

Changing ORU Network/Email Password

1. Log into http://vision.oru.edu.
2. Click on the Personal Information tab.
3. Click on the Create/Update Username, Password, and Email Address section.
4. Fill in **ONLY** the password fields.



Note: Please allow up to 10-15 minutes for the information to set in the system before attempting to log in.

Configure Mobile Device to Use Office 365 Email

Apple iOS (iPhone, iPad, iPod Touch)

Requirements

- iPad, iPhone, or iPod Touch
- An Office 365 Account

Configuration Steps

NOTE: If this is your first email account on your device, tap "Mail" and proceed to step 3.

1. Tap "Settings"
2. Tap "Mail, Contacts, Calendars" under Settings and tap "Add Account..." under Accounts.
3. Tap "Microsoft Exchange" under Add Account...
4. In the Exchange dialog box:
    - Enter your email address (e.g. username@oru.edu) in the "Email" field.
    - Enter your email address (e.g. username@oru.edu) in the "Username" field.
    - Enter your password in the "Password" field.
    - Enter Office 365 in the "Description" field.
    - *NOTE: You can use any short name that's meaningful to you, such as "ORU email".*
5. Tap "Next" in the upper right corner.
6. Verify the "Server" field was filled in automatically, then tap "Next" in the upper right corner of the Exchange dialog box.
    - *NOTE: If your iOS device is unable to automatically locate the correct Office 365 server name, please use outlook.office365.com for the server name.*
7. In the Exchange Account dialog box:
    - Choose the type of information you want to synchronize.
    - *NOTE: By default, Mail, Calendar, and Contacts are all turned on. You can turn off synchronization for any of these.*
8. Tap "Save" in the upper right corner.
9. Push the Home button on your device and tap "Mail" or "Calendar" to confirm that you've set up your Office 365 account information.

Android OS

Requirements

- An Android phone with access to the internet
- An Office 365 email account

Configuration Steps

1. Press the Applications Menu button and select Email.
    - *NOTE: The way to access email settings may vary depending on your type of phone.*
2. Tap Accounts & Sync in the Settings dialog box.

3. Tap Add account in the Accounts & sync settings dialog box.
4. Select Exchange account - this may also be called Exchange ActiveSync.
5. In the Add an Exchange account dialog box:
    - Enter your full Office 365 email address ("username@oru.edu") in the "Email Address:" field.
    - Enter your email password.
    - Tap Next.
6. In the Server Settings dialog box:
    - Enter your full ORU email address in the "Domain\Username" field.
    - *NOTE: If the Domain and Username are separate boxes, leave the Domain box empty and type your full email address in the Username box.*
    - Enter your email password in the "Password" field.
    - Use outlook.office365.com in the "Server" field.
    - Tap Next.
7. Your phone should now verify your server settings and open the Account Options display.
8. Select the settings that you want in the Account Options display and tap Next when you are done.
    - *NOTE: the options vary depending on the version of Android OS you have but may include: notifications, email sync times, and email push.*
9. Enter the Account Name you want to use - like "ORU Email".
10. Tap Done.
11. Return to your home screen and open your email application.
    - NOTE: You may have to force the email application to restart before you can use it.

Other Mobile Devices

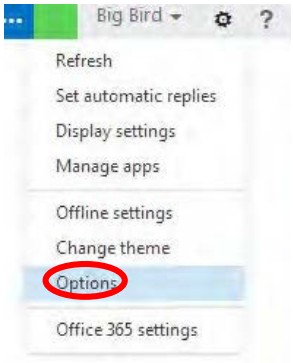
It may be possible for you to connect to Office 365 from additional devices not listed in these pages. Microsoft provides help with setting up many mobile devices for Office 365.

Microsoft Outlook Mobile Setup Wizard

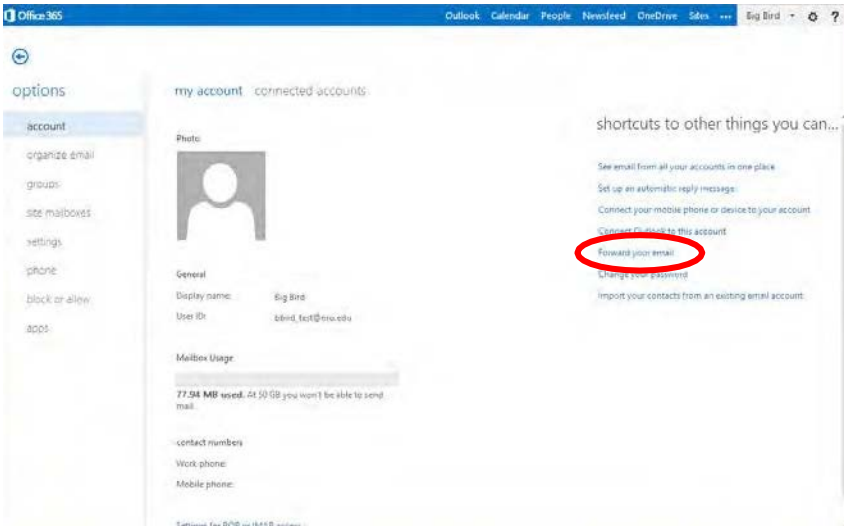
Forwarding Email from Office 365 to an External Account

1. Once you have logged in to your email account click on the "**Options**" link in the upper right corner of the screen to access your account settings.

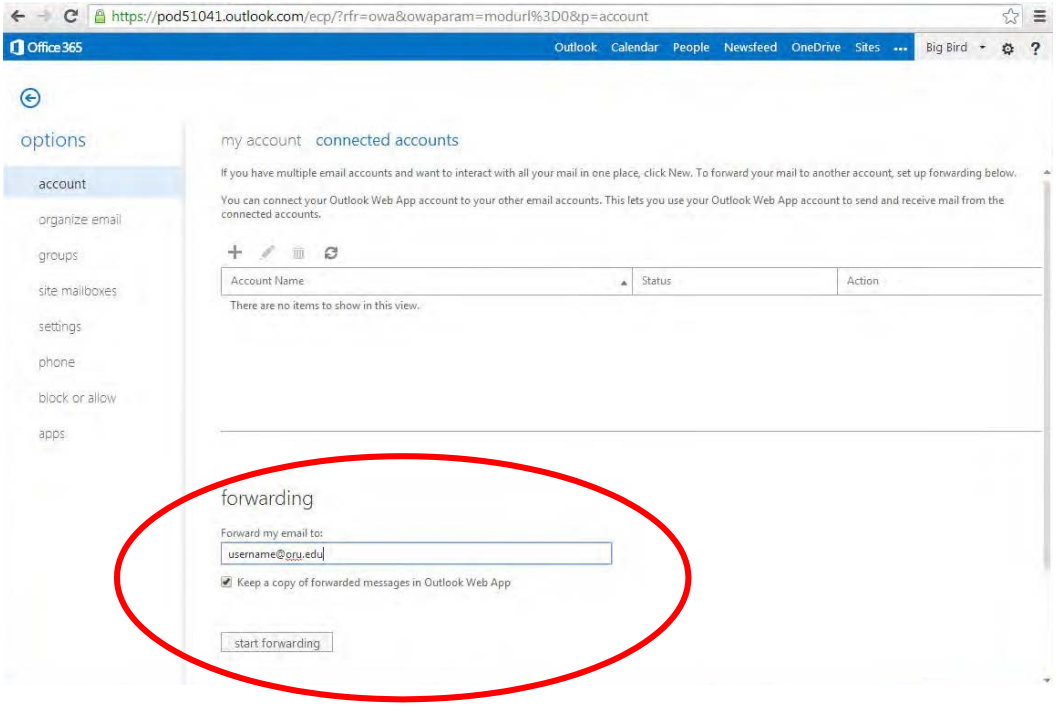
2. Choose "**Options**" from the dropdown menu.



3. On the "**My Account**" screen click the "**Forward your email**" button on the right side. This will be in the "Shortcuts to other things you can…" panel.



4. On the "**Connected Accounts**" screen type in the email address you would like to forward your mail to in the "**Forward my email to:**" section and click the "**Start Forwarding**" button.



NOTE: *The option to "Keep a copy of forwarded messages in Outlook Web App" should be checked if you want a copy to remain in the oru.edu account or unchecked if you do not want a copy to remain in the oru.edu account.*

Directions to the IT Support Locations & Academic Computer Labs

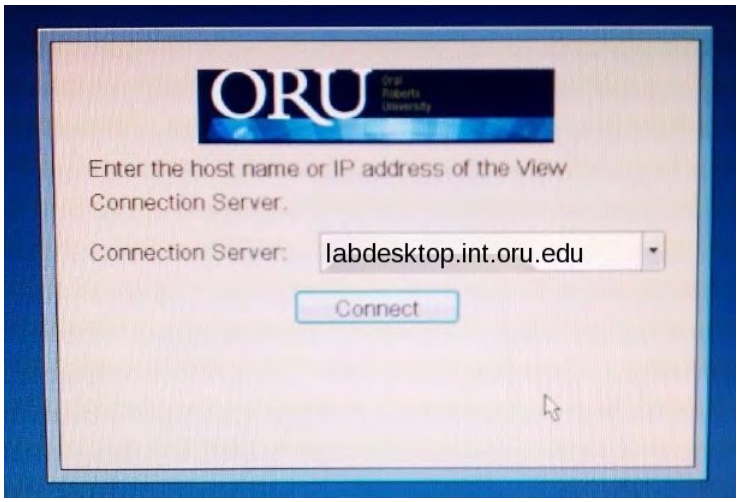
Academic Computer Labs

Located on GC 2 – when coming off the main elevators turn right and walk down the hallway. We have 3 computer labs located on GC2 – Labs 2 through 4 are used for classes and testing and are open for students when classes are not in session.

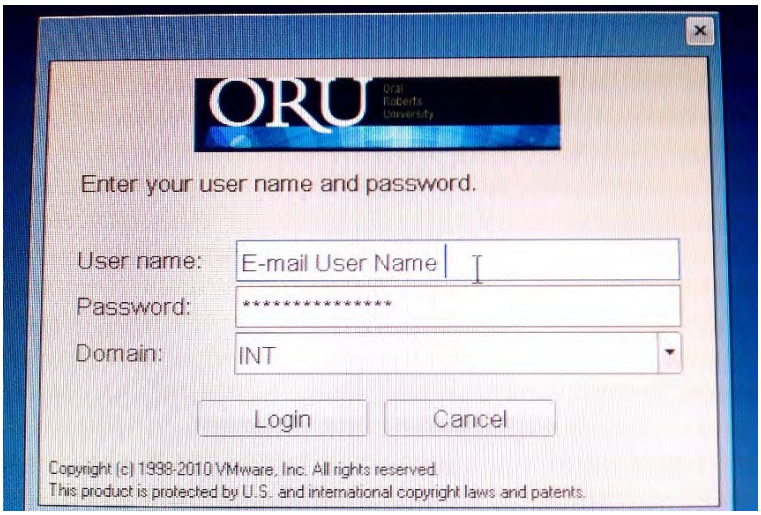
IT Customer Care Information Desk

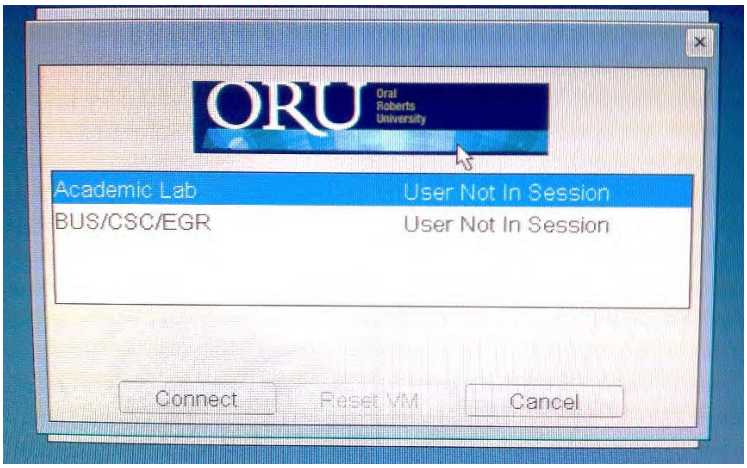
This is a general IT information desk located at the main entrance to the LRC/GC building on LRC 3 right outside Hava Java and the Admissions Welcome Center.

Logging into the Academic Computer Lab VDI Computers



1. Click the **Connect Button**
2. Enter your network username & password





3. Select "**Academic Lab**" and click "**Connect**"

ORU IT Personal Computer Repair Policy

An ORU ID (for active student or employee) must be presented before any work is done.
Users must be present while work is being performed on their personally owned computer.

We do not repair computers if brought in for the following reasons:

- User does not know password to log into the computer
- There is physical damage to the computer that is the cause of the problem
- If there is a hardware error which requires a hardware replacement

We will only support computers with the following operating systems:

- Windows 7 and above
- Mac 10.11 and above

What we provide:

- Assist in establishing a connection to ORU's wired and wireless network(s)
- Provide resources to download so that users can remove viruses, malware, or spyware from their computer systems.

  We regret that we are unable to perform virus, malware, or spyware scans on personally owned computers.

Requirements:

For ORU IT to evaluate a personally owned PC, it must boot up fully to the installed operating system and no hardware failures must be present. If the system is not operational, the user should either call the manufacturer for warranty repair or contact a computer repair facility.

Restrictions:

- Due to liability issues related to personally owned hardware, software, and data, ORU IT cannot perform hardware repairs on personally owned systems and will not install operating systems or application software.

- We will assist with installing school related software provided that the user has all necessary install files and any licensing codes needed for installation.
- ORU IT assumes no responsibility for personal data on a personally owned computer that is presented for repair. Users are responsible for backing up personal files.
- ORU IT cannot assist in the recovery or the re-installation of operating systems.
- ORU IT will not perform any service that voids a manufacturer's warranty.
- ORU IT reserves the right to not work on any personally owned computer that is dirty or otherwise hazardous. It is up to the user to provide ORU IT with a clean system prior to it being repaired.

As an education-based service, the helpdesk staff will educate you on technology and best practices if you are interested in learning.

ORU Web Filtering Policy – Why Some Sites are Blocked

The Higher Education Opportunity Act 2008 (HEOA), does not allow ORU to support/allow peer-to-peer file sharing on our network.

Several sections of the HEOA deal with unauthorized file-sharing on campus networks, imposing 3 general requirements on all U.S. colleges and universities:

1. An annual disclosure to students describing copyright law and campus policies related to violating copyright law.
2. A plan to "effectively combat" copyright abuse on the campus network using "a variety of technology-based deterrents".
3. Agreement to "offer alternatives to illegal downloading".

Please go to http://www2.ed.gov/policy/highered/leg/hea08/index.html if you want to read all the HEOA requirements.

Staying Safe on the Internet

Spam

Email spam, also known as junk email or email "phishing", is electronic spam involving nearly identical messages sent to numerous recipients by email. Clicking on links in a spam email may send a user to phishing web sites (where confidential information is asked for) or to sites that are hosting malware. Spam email may also include malware as file attachments. Phishing emails are designed to trick you out of sensitive information like passwords and account numbers. They are designed to appear as though they come from legitimate businesses. Many of them claim to be conducting an audit and may ask for your password or account numbers for authentication.

While much of spam is sent to invalid email addresses universities and corporations can be targets of spam since they have large numbers of email addresses that use a similar naming scheme.

To address this growing challenge with spam, we currently utilize a spam filtering software package called BARRACUDA. This gives us a tool to better manage our email system while at the same time giving you, our users, a great deal of control over your own email. It does this by filtering out a large majority of spam messages but still allowing you a way to create a personal "white list" so important emails don't get snagged by the filter. While this software does filter out a large majority of the spam we receive you may still get some spam messages in your inbox.

ORU IT will **NEVER** request sensitive personal information by email – this is also true of many legitimate businesses. If you ever receive an email that you find suspicious, please do not click on any links. Instead, you can contact helpdesk@oru.edu and ask about the suspect email.

Things to Keep in Mind about Email "Phishing"

There are a couple of things to keep in mind to determine if an email you have received is fraud:

- **Sender's Address** – phishing emails may show a real email address; con artists will often edit the "From" line prior to sending out their email.
- **Email Greeting** – many phishing emails will start with a general greeting as the con artist does not know your name.
- **Account Status** – most phishing emails will try to deceive you with a threat that your account is in jeopardy or that it is being updated.
- **Links in an Email** – While legitimate emails will include links, phishing emails will try to redirect you to the con artist's site instead. You can spot a forged link by rolling over the link with your mouse and viewing the real location in the pop-up bubble or at the bottom of the reading pane.
- **Requests for Personal Information** – Phishing emails often include requests for sensitive personal information like usernames, passwords or bank account numbers. Keep safe by never revealing information like that through an email request.
- **Misspellings & Grammatical Errors** – Many times when a phishing email is sent, it may have logos or links that make it look like an email from a legitimate source, but you will still see misspellings or grammatical errors in the email itself – including sometimes the name of the "company" sending you the email.
- **Still not sure if it's legit?** You can always do a search on the internet for thekeywords from that email along with the word "spam" to see if the email you received is legitimate or if that company has published anything warning users about spam.

Potential Risks

Non-secure data

Anything transmitted over a website that does not start with **https://** is not secure and the data can be easily read by an attacker on the network with simple tools that can be downloaded for free.

Man in the middle attack

This type of attack is particularly popular in foreign countries. When you put the web address into your web browser *i.e. bankofamerica.com*, the web browser goes to DNS (Domain Name Servers) to get the IP address for bankofamerica.com which would be 171.159.228.150 – this is how your computer gets to the webpage.

An attacker can pretend to be the DNS server and redirect you to another website that may look exactly the same as the destination you are trying to reach – in this example bankofamerica.com. The attacker can steal your username and password and have access to your bank account or whatever website you are trying to log in to.

Shared files can be viewed

If when connecting to a public network, home network or work network is accidentally selected on Windows, any files in the public documents, public pictures, and public music can be viewed by anyone on the network.

Best practices to avoid these attacks

Connect to secured networks if possible

Secured networks require a password and are therefore safer because of limited access.

Secured network on Windows *Secured network on OSX*

Only connect to networks you trust

If you are in a public area, only connect to a network if you know from where it is being broadcast. For example, if you are at a Starbucks, do not connect to a network that is called McDonalds. Also, avoid networks that are named things like “Free Public Wi-Fi” or “Starbucks FREE.” If you are unsure, **do not connect**. Asking the employees of the coffee shop, hotel, or airport how to connect to the network may help you decipher if a network is legitimate or not.

Do not use Public Wi-Fi for online banking or shopping!

Protect Your Passwords

Using unique passwords for different accounts can help if one of your accounts is compromised. Keeping track of multiple secure passwords can be tricky, so using a password manager such as KeePass or LastPass can help keep you safe and secure.

Both KeePass and LastPass are free, but they store your information in different ways. KeePass keeps an encrypted database file on your computer, while LastPass stores your credentials in the cloud. There are pros and cons to each approach, but both services are completely secure.

Use passwords that are not easily guessed.

Avoid letting the browser remember passwords on websites.

Use Two-Factor Authentication

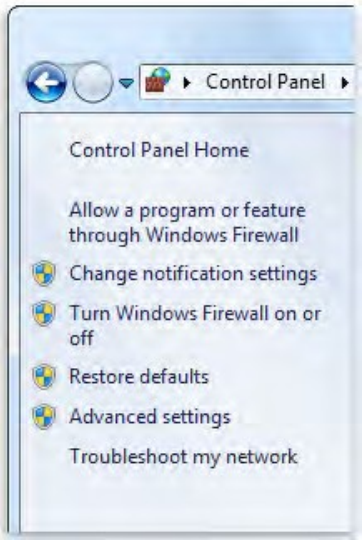
Two-factor authentication means you need two pieces of information to log into an account: One is something you know and the other is something you have. Most often this takes the form of a password and a code sent to your cellphone.

Many popular websites and services support two-factor authentication. This means that even if someone is able to get your password due to a hole in a public Wi-Fi network, they won’t be able to log into your account.

Turn on Your Firewall

Most OS's include a built-in firewall, which monitors incoming and outgoing connections. A firewall won't provide complete protection, but it's a setting that should always be enabled.

On a Windows notebook, locate your firewall settings in the **Control Panel** under **System and Security**. Click on **Windows Firewall**, then click **Turn Windows Firewall On or Off**. Enter your administrator password, then verify that the Windows Firewall is on.



The settings on a Mac are in **System Preferences**, then **Security & Privacy**. Navigate to the **Firewall** tab and click **Turn on Firewall**. If these settings are grayed out, click the padlock icon in the lower left, enter your password, and then follow these steps again.

Run Anti-Virus Software

Always running up-to-date anti-virus software can help provide the first alert if your system has been compromised while connected to an unsecured network. An alert will be displayed if any known viruses are loaded onto your PC or if there's any suspicious behavior, such as modifications to registry files.

While running anti-virus software might not catch all unauthorized activity, it's a great way to protect against most attacks.

Security browser extensions

One essential browser extension recommended is HTTPS Everywhere from the Electronic Frontier Foundation (EFF). This allows you to have a secure connection when you visit common sites like Google, Yahoo, eBay, Amazon, and more. It also allows you to create your own XML configuration file to add more sites not listed.

It's available for both Chrome and Firefox and works with Windows, Mac, and Linux.

Keep your software updated

Finally, it's important to ensure your antivirus and malware protection is up-to-date, as well as your operating system. Operating system updates not only keep your system running smoothly, but they also

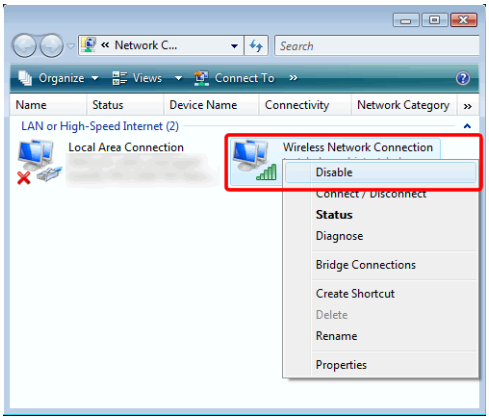
patch security holes. Keep in mind that nothing is 100 percent secure on the internet. But the more layers of security you add, the better protected you'll be.

Be extra careful about the sites you choose to visit.
Read carefully before choosing to click on pop-ups.

Turn Wi-Fi Off When You're Not Using It

If you want to guarantee your security and you're not actively using the internet, simply turn off your Wi-Fi. This is extremely easy in both Mac and Windows.

On a Mac, just click the **Wi-Fi icon** in the menu bar and select the **turn AirPort off** option.



On Windows, you can just **right-click on the wireless icon** in the taskbar to turn it off. You can also go into your Network Connections and **right-click** on the Wireless Network Connection.

Again, this isn't all that useful if you need the internet, but when you're not actively using it, it's not a bad idea to just turn it off for the time being. The longer you stay connected, the longer people have to notice you're there and start snooping around.

Keeping your Laptop Safe

- Never load passwords on the laptop, particularly those allowing remote and email communication.
- Consider installing a boot-up password.
- Back up your files and carry them somewhere other than the laptop.
- Never leave your laptop unattended in a public place, even for a moment.

- Pay attention to where you use your laptop as there could be those behind you observing your screen.

Anti-virus & Anti-malware Protection

Oral Roberts University IT recommends that you install and use both a good anti-virus program and anti-malware program. There are several options available – both paid and free – but anti-virus combined with a good anti-malware program are essential to protect both your computer and your data.

One of the anti-malware programs that we highly recommend is Malwarebytes (https://www.malwarebytes.org/). It's both easy to install and easy to use.