

Olympia Technology Department Technology Issues

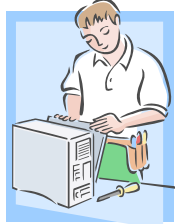
TOPIC: SECURITY

Security is critical. For one thing, you try to keep your body secure from illness. You wash your hands as a preventive measure and you take precautions not to “catch” anything when you are near people who you can tell are sick and maybe contagious. Personally and through the media, doctors provide you with warnings and advice on how to be as safe from harm as you can be.



But the doctor can only do so much to help protect you. That doctor has to rely upon you to protect yourself and do what is smart and healthy. You can choose to kiss somebody with the flu, then take a drive at 90 mph while talking on the cell phone and eating a burger – ultimately, it is in your hands. *It isn't the doctor's responsibility to make sure that you can't get sick or injured.* **Everyone knows that would be impossible.**

Another kind of security concern affects your need here at Olympia to have the use of technology tools to do your job. The computers and the network need to be dependable. In order to provide that dependability, the technology team continually tries to provide you with tips and suggestions that will help you maintain network security.

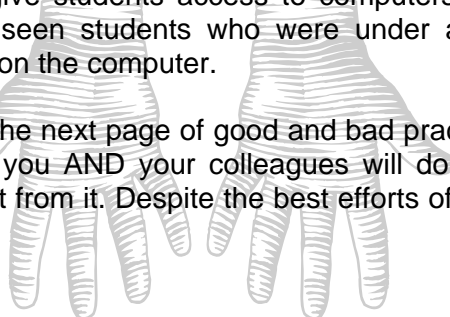


But the tech team can only do so much to help protect you. We have to rely upon you to protect your account and do what is smart to keep the entire network healthy. You might choose to log into your computer and then leave it unlocked and unwatched and you could ignore students that are clearly visiting inappropriate websites and downloading potentially harmful files - ultimately, the security of Olympia's network is in the hands of its users.


It isn't the tech team's responsibility to make sure the computers and the network can't be harmed. **Everyone should understand that is impossible.**


We are thankful that many staff members practice good network security. Our network has provided us with a lot of good service this year; it's evident that we have plenty of users keeping security in mind. But we have had multiple instances this year where staff members have willingly or carelessly allowed students access to the network with staff level privileges. We have seen staff members give students access to computers and walk away and numerous occasions where we have seen students who were under adult supervision but who were unmonitored in their actions on the computer.


Please take a close look at the next page of good and bad practices and ask yourself if you are following the good ones. If you AND your colleagues will do that, we will all be much more secure and we will all benefit from it. Despite the best efforts of the technology team, *ultimately, it is in your hands.*





 = Good  = Bad


 Every time you log in to the computer, you make sure that no one is watching your hands or the keyboard.


 With students standing around you, you log in to the network by typing your password with one finger, one key at a time.


 You have logged into the computer but you need to leave the room, perhaps to supervise recess or an assembly. You use “Ctrl – Alt – Delete” and select “Lock computer” knowing that when you return it is simple for you to hit “Ctrl – Alt – Delete” again, enter your password, and you are back in business without delay.


 You have logged into the computer but you need to leave the room. Since it is too inconvenient to lock it and unlock it and you can't imagine any of the students would ever do anything they shouldn't, you walk away leaving your network account wide open to anyone who might step up to the computer.


 A student says he can't access a website that he needs for an assignment. Alone, you check the website to see if there is anything obviously objectionable. You don't see anything wrong, so you put in a Tech Work Order requesting the site be unblocked.


 A student says she can't access a website that she needs for an assignment. With the student at your side, you log in to your account, call up the website, let the student take your seat, tell her you'll be back soon and leave the room.


 In the lab for research with your class, you see a student looking at a web page that isn't appropriate for his assignment. You direct him to get back on task and watch him more closely the rest of the period.


 In the lab for research, you see a student looking at a game website that isn't appropriate for his assignment. Seeing he is entertained and non-disruptive, you decide not to confront him but the next time you see a tech team member you make sure to say, “You need to do a better job of blocking games.”


 You change your password at least twice a year. You select a password that is at least 8 characters long and includes letters, numbers, and symbols. Exs.: !Maii*87, 19&Oly\$94. You share it with NO ONE, not even your mom.


 You are proud to say that you have had the same password for more than 3 years. It is the name of your pet/child/spouse. You make a habit of telling your students that your password is the name of your pet/child/spouse. You have pictures posted in your room of your pet/child/spouse with their name on them.


 You are cautious about ever writing your password down and if you do, you keep it in a secure (locked) location.

 Knowing that you will have a sub tomorrow, you write your username and password on a piece of paper and put it in your unlocked desk drawer. You leave an open note for the sub on your desk with instructions including where to find your password.

 You receive an email with an attachment; you don't know the sender and/or are not sure what is in the attachment. You either delete it promptly or, if you think it is legitimate, you right-click the attachment to save without opening it first, right-click on the saved file to scan it for viruses and only open it after finding it safe.

 Whenever you receive an email with an attachment you open it right up. It doesn't matter who sent it or if you have any idea what it is, you just want to see what's inside.

 Preparing for a lesson, you find a web site that you want to use with students. To be sure they can access it you log in as a student and make sure it isn't blocked. If there is a problem, you let the tech team know about it at least a couple days in advance. [To get a student log-in, check with your building's tech team member and please keep it secure.]

 Preparing for a lesson, you find a web site that you want to use with students. The day of the lesson, you take the class into the lab and direct them to the website. It is blocked for students so you call for a tech team member and demand the site be unblocked immediately. You blame the tech team for wasting your time.