Berlin Public Schools

April 2019

Technology Department Newsletter

2-Step Verification

If you haven't set up 2-Step Verification please do it now.

Click here to set it up: 2-Step Verification

(if you need help, put in a ticket)

Tech Committee Meeting Dates
All Are Welcome

April 8, 2019

Website Unblock Request Link

Here is the URL for the Unblock Website Request Form. Please share this link with your students.

GoGuardian Update to Scenes

Click here for more info.

Please don't hesitate to contact us with any questions!

DO NOT SHARE PASSWORDS:

Under any circumstances, please do not share your passwords with others, including all staff and substitutes. Passwords such as laptop, Gmail, PowerSchool, etc should never be given to someone else.

In the event you are having an issue, and the Tech Department needs your password to solve the problem, we will come see you in person and will never ask for it in an email.

Malwarebytes:

Do to the increased number of viruses and malware attacks this year, we are implementing new software on all PCs (not Chromebooks) called "Malwarebytes" to combat and protect us against these attacks. You may see a small icon  in the bottom right hand corner of your taskbar. We will be running scheduled scans of your device, but you can initiate a scan yourself by right clicking the icon and selecting "Start Threat Scan."

Removed Sync on Personal Devices for Students:

The new state law concerning student privacy unfortunately requires us to restrict access to the Google Suite Apps on personal devices to comply with students privacy rights.

Students will not be able to connect to Mail, Google Drive, Classroom, or Docs on their phones or tablets through the apps, but most G Suite Apps can still be accessed through the browser (Safari, Chrome, etc) on their phones.

All school work (Classroom, Drive, Docs, Mail, etc) can be accessed from any PC, MAC or Chromebook.

Email/ Phishing:

Please continue to be vigilant when it comes to suspicious emails. **We will be conducting email phishing tests periodically throughout the rest of the school year.**

When you get an email that looks suspicious, here are a few things to check for:

- **Check that the email address and the sender name match.**

- Check if the email is authenticated.
- Hover over any links before you click on them. If the URL of the link doesn't match the description of the link, it might be leading you to a phishing site.
- **Check the message headers to make sure the "from" header isn't showing an incorrect name.**