Technology Department Newsletter

Please put in a HelpDesk Ticket for any problems you have.

Continue to Check SDPC

- Friendly reminder to continue to check the Student Data and Privacy Consortium website before using tools and resources with your students. To see a full list of the approved tools please visit the SDPC Resource Registry for SAU3. To check other NH approved tools, you can search the State Resource Registry. This is a great resource to find already approved tools if the one you are using is not approved.

- Only resources that say ACTIVE in the Agreement Status column can be used.

<table>
<thead>
<tr>
<th>Resource Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kahoot!</td>
<td>Active</td>
</tr>
<tr>
<td>Quizizz</td>
<td>Active</td>
</tr>
<tr>
<td>Quizlet</td>
<td>Vendor Unresponsive</td>
</tr>
<tr>
<td>Classmarker</td>
<td>Not Approved</td>
</tr>
</tbody>
</table>

- If you do not see a resource you want to use on the Berlin Public School Registry list, please put in a helpdesk ticket with the name and URL of the resource and we will submit it for approval.

Zoom/GoGuardian Teacher

- The Zoom app has been removed from the Chromebooks now that we are no longer remote. However, it is enabled for any students taking the remote VLACS path.

- GoGuardian Teacher has new video conferencing features that allow teachers to voice or video call students being monitored remotely. It is our recommendation to use this feature for students who are temporarily remote. You can find this feature under the Call Students tab of your GoGuardian Teacher dashboard.

2-Step Verification
Set up 2-Step Verification

1. Go to the 2-Step Verification page. You might have to sign in to your Google Account.
2. Select Get started.
3. Follow the step-by-step setup process.

Once you're finished, you'll be taken to the 2-Step Verification settings page. Review your settings and add multiple verification methods.

After the initial setup, you may print out a list of codes that can be used as an alternative to receiving the codes on your phone.

**Note: Initial setup needs to be done on a PC, not a Chromebook.**

Due to new security requirements by Primex, our insurance provider, 2-Step Verification will be mandatory starting December 11th. Please set this up before then, and if you need help let us know.

Passwords

Primex is also requiring everyone to change and update their passwords at least twice a year. This includes both Gmail/Chromebook and computer/laptop logins. If you have not changed your password recently, we recommend you do so now.

Instructions for Gmail/Chromebooks:

- Click this link: [https://myaccount.google.com/u/0/security?hl=en](https://myaccount.google.com/u/0/security?hl=en)
  - If you are not signed in, you may need to sign in with your SAU3 email
  - Under Signing in with Google, click Password
  - Sign in using your current password
  - Type in your new password

Instructions for computers/laptops:

- Sign into the laptop
- Press CTRL + ALT + DELETE
- Select Change a Password
- Type your old password once, and your new one twice
  - Make sure it is 10 characters, including upper case, lower case, number, symbol

KnowBe4

For those who are new to the district, KnowBe4 is a security awareness training platform. We regularly send test phishing emails through KnowBe4 and provide security training modules through the online portal.

To login to the online portal and view the trainings, go to [training.knowbe4.com](http://training.knowbe4.com)
Enter your email and follow the prompts to login

- These trainings are not required, but are recommended and do count towards your PD CEUs.

From Primex:

**Business Email Compromise Bulletin**

Business Email Compromise (BEC) is a type of cyber-attack that is largely successful due to a reliance on email to conduct personal and professional business. Criminals send users an email message that appears to come from a legitimate source making a legitimate request. Clicking on a link, opening an attachment, or providing login information when prompted can allow the attacker to enter your computer and network. This provides undetected access to company financial accounts, calendars, and protected data that gives criminals the details needed to carry out the attack.

Look for attackers to spoof an otherwise familiar email account or website. There may be slight variations on legitimate addresses to fool victims into thinking fake accounts are authentic. For example, thomas.williams@localgovernmententity.org may be replaced with thomas.williams@localgovernmententity.org.

Also, be wary of opening attachments from unknown or unconfirmed sources. These types of attacks often begin with a phishing email conveying a sense of urgency. In today's busy world, it can be common to rush when reading and responding to emails. Remember to SLOW DOWN, STOP and VERIFY the authenticity of the email and the transaction by communicating through a known telephone number or email address.

**How can you prevent BEC?**

1. Train and educate employees on how to detect phishing emails.
2. Create an approval processes when making invoice payments or financial transactions. Having this secondary authorization can mean the difference in paying a trusted vendor or having money stolen by a cyber-attacker.
3. Require verification before making financial transactions. Always use known contact information (phone or email) prior to the authorization of funds being transferred.
4. NEVER share your password or passphrase with anyone.
5. Create a collaborative culture that encourages employees to report suspicious email or other communications.

Taking a little more time when reviewing emails, creating secondary or supervisory approval requirements for financial transactions, and verifying payment requests through known contact information can better protect your organization from BEC.

For more information, please contact Cori Casey, Risk Management Consultant at 800-696-2364 x 118 or email ccasey@nhprimex.org.

800-696-2364
46 Donovan Street, Concord, NH 03301


www.nhprimex.org