VERMONT
AGENCY OF EDUCATION
CHILD NUTRITION PROGRAMS

1 National Life Drive, Davis 5, Montpelier, VT 05620-2501
(p) 802-828-1626 | (f) 802-828-6433
education.vermont.gov/student-support/nutrition

Helpful Security Tips

Passwords

Passwords are one of the most important factors in keeping your email information safe. A good strong password is the first level of defense against a security breach. Don't use generic passwords. Things like CompanyName123 and FirstLastname! aren't secure – especially when it comes to admin level accounts. To make sure things stay secure, change your passwords often, and use a different one for each account. Also make sure not to share passwords – even with members of your own team.

Phishing

It's important to learn how to recognize phishing emails because they can extract personal information and install malware on your system. Phishing emails may contain threats to shut your account down, have poor grammar, and use words like 'urgent' to get you to give them sensitive information or click on a link that leads to a harmful download.

A reputable business will never ask for sensitive and personal information via email. If a message asks for things like passwords or social security numbers, this should put you on high alert. Make sure to check the sender's email address. Is it forged? Are there misspellings? Do links in the email lead to a questionable source?

At first glance, a link like yourbank.example.com might look like it leads to a page on yourbank.com, but it's actually a completely different domain. A simple way to check the links is to hover over them to make sure they look legit before clicking on them. It's also a great idea to make sure that all sensitive data within your organization like credit cards and social security numbers are stored on a private encrypted volume that has limited user access (perhaps only HR).

Attachments

Attachments are another method to get access to your data. Before opening an attachment, make sure that you know who it's from and that you are expecting it. Save the large files (anything over 1 or 2 MB) for something other than email, like Google Drive or Dropbox. Always make sure to scan all attachments with a good antivirus software program before opening and be especially aware of any zipped attachments, ones with unusual file types, and Office documents with macros. Scammers use all of these tactics to install malicious software on your machine.

Security

In addition to all of the above, general security measures can also be effective against malicious attempts. Don't send any personal information over email and make sure that your mail provider uses SSL or TLS to make sure that your email is encrypted from the time you hit the send button to when it shows up in the recipient's mailbox. Keep user drive permissions locked down and secure. Even personal laptops that aren't managed by your organization might already be infected and could even have networked drives mapped. Make sure that security software is up to date.

Educate

Email security doesn't need to be complicated but it's one of those things that is necessary to talk about. The consequences can be drastic and it's worth having a proactive plan of protection. Education is the most important aspect in keeping your organization safe. Make sure everyone knows the above precautions and how to handle their email security.

Check out this Keep Your Email Secure: Best Practices Cheat Sheet for more helpful email security tips.