



May 2018

# INTERNET & EMAIL SAFETY



## PRACTICE SAFE BROWSING

Make sure you are visiting safe websites with the correct URLs and be careful not to click on suspicious links on websites.

## BE MINDFUL OF YOUR EMAILS

If the email looks suspicious or is asking you for personal information or wire transfers report it to a member of the technology department immediately.



## PASSWORD SECURITY

Please make sure your passwords are secure, complex, and not in plain sight. This means passwords should include upper and lowercase letters, numbers and symbols. Passwords should be strong and unique. Please do not leave your password taped to your computer, laptop or desk.

\*\* Do not use the same password for all sites.

## SECURE YOUR COMPUTER

Lock your computer when you leave the room so no one can view what is on your screen



# THINK BEFORE YOU CLICK

Pause before opening attachments in email, even if you think you know the sender, they could be harmful.



## BACK UP YOUR DOCUMENTS

Back up information that is irreplaceable. Information should be saved to your designated server, not your computer. If you need assistance or directions with this, please submit a support ticket.

## SOCIAL MEDIA AWARENESS

Be careful about what information you are posting to social media accounts. Always maintain separate professional and personal accounts.

## BE WARY OF SOCIAL ENGINEERING

When someone attempts to gain information through phone, email, or text message. It is okay to tell them no, you can check with a technology member first if you are uncertain.

## KEEP YOUR GUARD UP

Always be cautious about what you do online, which sites you visit, and what you share.



HAVE A QUESTION?  
NEED TRAINING?



THINK YOUR ACCOUNT HAS  
BEEN COMPROMISED?

## SUBMIT A SUPPORT TICKET

Or email one of the Tech staff!

Visit [http://www.fairhavenps.org/our\\_district/technology](http://www.fairhavenps.org/our_district/technology)

