CQC - Cybersecurity

Randy Mills M.Ed.
Project Lead The Way Master Teacher

TOP TEN BEST PRACTICES

1. Create Passphrases and make them strong
2. Secure Access to accounts
3. Think before you act
4. When in doubt, throw it out!
5. Share with care
6. Use security software
7. Adjust browser safety settings
8. Use default firewall and security on your machine
9. Log out
10. Consider support

SOURCE: https://www.protectseniorsonline.com/resources/cybersecurity-best-practices/

Pass Phrases

Create a sentence that is complex. For example:

Myfootballnumberwas#3

Use Password Software

LastPass

Master Password

Create a complex Passphrase for the account

Use complex passwords on the individual site.

Let LastPass navigate the different sites

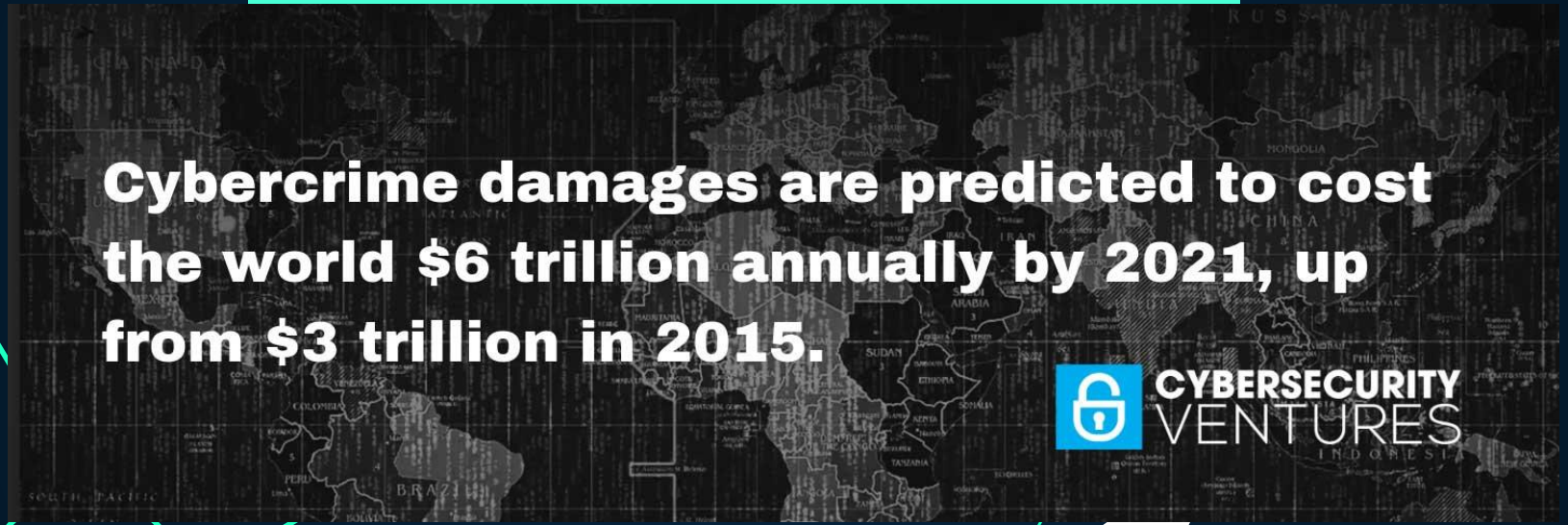
2 Factor Authentication

Use a program not your text message system

Phishing - 91%

1. Legit companies don’t request your sensitive information via email
2. Legit companies usually call you by your name
3. Legit companies have domain emails
4. Legit companies know how to spell
5. Legit companies don’t force you to their website
6. Legit companies don’t send unsolicited attachments
7. Legit company links match legitimate URLs

Source: https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email


Cybercrime damages are predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.
CYBERSECURITY VENTURES

When in doubt:

Call the Sender

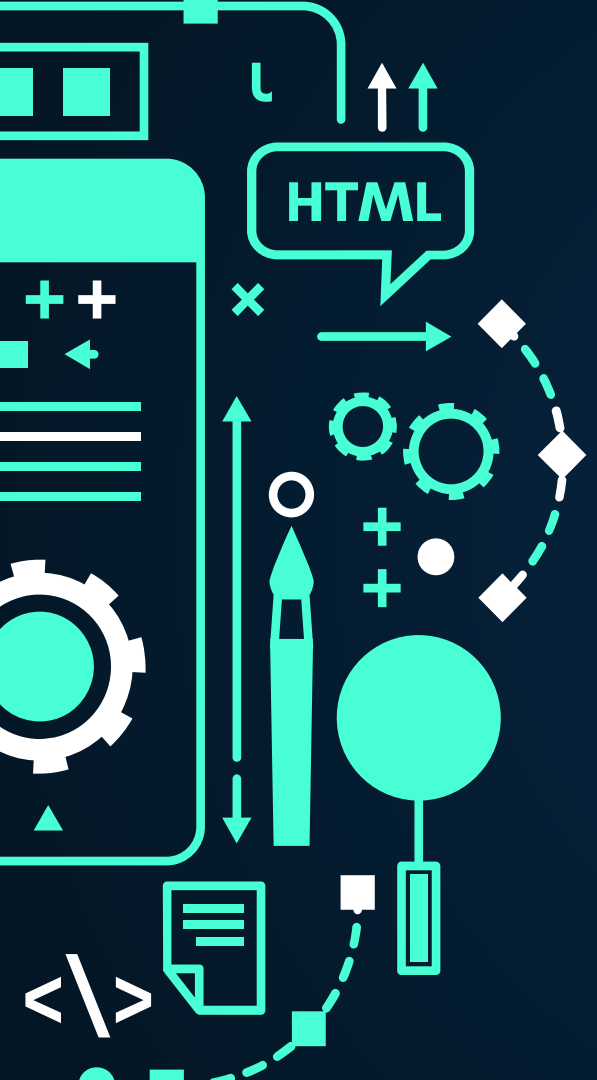
If you don’t know them throw it out

Seek an expert

Don’t take anything for granted

A legitimate company/friend will not mind answering the inquiry

Do not click on links or open attachments unless you are sure if the are valid.



THANKS!

Does anyone have any question?

RDMILLS@aurorak12.org
RDMILLS.aurorak12.org