FCS Technology Services

Our staff is the first and best line of defense against cyber attacks.

The FCS Technology Services department would like to welcome you and share some simple things you can do to help protect the district and allow you to #BeCyberSmart.

Hacking – Not What You Think

When one thinks of hacking, perhaps an image of a hooded figure – hunched over a computer in a dark room – comes to mind… or images of fast-changing characters flash in the mind's eye. However, most attacks are much more mundane since they target a highly vulnerable asset: the end user.

Indeed, a majority of the 1,473 reported corporate breaches in 2019 (a 17% increase over 2018) gained a foothold on the network through human error. While billions of dollars have been spent globally on hardware and software solutions, the human element is the one mostly responsible for the loss of confidential data.

> *You should NEVER share your password with anyone, and no one from FCS should ever ask for your password.*

Tips

Thankfully, the “fix” for this vulnerability is inexpensive – and, thankfully – easy to implement. To that end, here are the things you can do in order to #BeCyberSmart:

- **Don’t mix your personal and private business.** Though it is convenient to use one email address for electronic communication, doing so greatly enhances the likelihood of a breach. You should never use your FCS email for personal correspondence, nor should you ever use your personal address for official FCS business. Don’t share confidential information over email; instead, use the Secure File Transfer system provided by FCS.
- **Protect your password.** You should NEVER share your password with anyone, and no one from FCS should ever ask for your password. Additionally, never use the same password across multiple services. Lastly, you should always use a complex password. A proper sentence – with capitalization and punctuation – is generally very complex and difficult to crack. Never write your password on a note and leave it on/near your computer.
- **Look for clues.** If you receive an email that looks like it came from an FCS employee, but has a banner message stating that it’s an external sender, be skeptical of it. Also, phishers – people who attempt to hack through social engineering – are often from countries who do not natively speak English. If the spelling or grammar is poor, that can also be a key indicator that it isn’t legitimate.
- **Do you trust that attachment?** If you’re not expecting an attachment from someone, then don’t open it without verifying its nature. If you know the sender, contact them directly (don’t reply to the email) and ask if they sent the email.
- **Don’t click the link.** Phishers will also try to steal your information by giving you a URL that asks for your credentials. Once they have that, they have full access to your account.

- **Unity** – Submit a Unity ticket when you are having Technology issues at the following link https://unity.forsythk12.org/ and a Technician will arrive for assistance.
  ***Note- Check with the ITS at your FCS location to see how they want to handle Technology assistance. Some may want to help if free, while others may want you to submit a Unity ticket.**

- **Email** – How to access your FCS email on non-Forsyth County School devices, visit http://classlink.forsythk12.org/ , select the *O365* app or the *Teacher Tools* app, then click *Outlook 365*.

- **Copier Access** – All FCS copiers require badge access, if your FCS badge does not allow you to copy documents, email Whitney Kelley in Technology Services at wkelley@forsyth.k12.ga.us.

- **How To Videos** - Visit https://www.forsyth.k12.ga.us/Page/52256 to check out helpful tips on using Microsoft Teams, Outlook, O365, Power BI and PaperCut.

Technology Services Contact Information
Whitney Kelley
wkelley@forsyth.k12.ga.us
770.887.2461 ext-202261