Despite its "interesting" start, I am still optimistic that the year ahead of us will be a vast improvement over the year that is behind us. As a matter of fact, I’m going to go out on a limb here and say, “Hey, it can’t be any worse!”

With that in mind, I wanted to let you know about two things have recently come to my attention:

**DUO swarms.**
This is a rather effective method used by attackers to get past the multi-factor authentication step.

**Facebook 2019 data exposure.**
In late 2019, everyone’s favorite social media site managed to expose a database filled with user data. Specifically, names and phone numbers.
DUO swarms.
This attack is simple and highly effective.

An attacker who has successfully phished your login and password information still needs to get through the multi-factor step in order to gain access to your account. They do this by sending a barrage of DUO login requests to your phone until you finally get annoyed enough and out of sheer frustration, you approve the request in order to get them to stop.

Should you ever begin to receive DUO access requests that you did not initiate, this is an indication that someone other than you probably knows your password. You should change it as soon as possible. As a matter of fact, you should change it immediately and if you used that password on any other account you have, you should change it on there as well.

Facebook 2019 data exposure.
Get ready for targeted phone calls.

In 2019, Facebook inadvertently left a server exposed on the internet and someone was able to download a database of Facebook user information. While the majority of the data is meaningless, it did contain the name and phone number associated with every account.

Recently, someone has begun selling the names and phone numbers from that database. This means that if you had a Facebook account in 2019, you may begin to receive phone calls where the caller knows your name and uses it to gain your trust or convince you of whatever they are trying to convince you of.

For instance, those ongoing attempts to scam you out of money by telling you there is an arrest warrant in your name become a bit more convincing if the caller actually knows your name.

When it comes to phone calls or emails that you receive, my advice to everyone is to err on the side of caution.

- Be wary of phone calls that are unexpected or claim to be from an authoritative government agency.
- Never give your personal information to anyone who calls you.
- If someone calls you and demands you provide them with gift cards to clear up a legal matter, hang up your phone. No government agency is ever going to demand payment in iTunes gift cards.

I firmly believe there are brighter days ahead and I, for one, plan on enjoying them.

You should plan on enjoying them as well.

For more ITS resources and information, please visit support.baypath.edu

If you have any questions or need help with technology, please feel free to contact the Help Desk by email (techsupport@baypath.edu) or phone (413-565-1487).