This is more information on a previous email I sent last week in regards to increases in phishing and security scams (see #4 below). This one comes from Education Week. Please be extra vigilant and remind students of this as well. Do not share any of your school account passwords or information etc. thank you.

Coronavirus Compounds K-12 Cybersecurity Problems: 5 Areas to Watch

By Jake Maher

March 17, 2020

Cybersecurity experts have warned about **coronavirus** pandemic-related phishing scams targeting all sectors of the economy, from health care and consumer products to banking. Now, schools are being warned to be extra vigilant too.

Doug Levin, the founder and president of the K-12 Cybersecurity Resource Center, pointed out that schools have long been the subject of "drive-by" phishing scams: mass blasts of dubious emails looking to gather personal information. In recent years, they've also been hit with more sophisticated and targeted attacks.

The coronavirus pandemic, Levin said, compounds the problem.

"Scammers and criminals really understand the human psyche and the desire for people to get more information and to feel in some cases, I think it's fair to say in terms of coronavirus, some level of panic," he said. "That makes people more likely to suspend judgment for messages that might otherwise be suspicious, and more likely to click on a document because it sounds urgent and important and relevant to them, even if they weren't expecting it."

Here are 5 takeaways from a recent conversation Educaton Week had with Levin.

1. Remote Classes Can Make Schools More Susceptible

Moving to remote classes is an important step in promoting social distancing in order to limit the coronavirus' spread, but having students and teachers access schools' networks remotely also increases the potential for an attack, according to Levin.

"With more teachers and students online, particularly if they're doing it from less controlled environments outside of the school, the attack surface of the school community is increased," he said.

"In many cases, all it takes is for one person to make a mistake in a school community for a school district network to get infected, or a data breach to happen."

2. Don't Count on the Same Level of IT Support as Usual

Another challenge of a large number of students and teachers working remotely is that the increasing number of IT problems associated with e-learning will divert resources away from cybersecurity. Schools, Levin said, also tend to have older IT infrastructures, and staff that may not be as highly trained in cybersecurity as people in industries such as banking and healthcare.

If IT staff members have to work remotely, and maybe also have to deal with a flood of low-level tech support issues, they are going to be able to be less attentive to incidents as they start to emerge, according to Levin.

Hackers often pick chaotic times or moments when schools' defenses are down, like spring break or the time right before school starts, to attack, Levin added. The coronavirus pandemic is a large enough social disruption to attract that kind of attention.

3. Even Small Schools Aren't Safe

A common misconception, Levin emphasized, is that smaller schools are safer because hackers don't think it's worth their time to target districts with only a few students.

“Based on the evidence I’ve seen about school cybersecurity events, the criminals and the scammers absolutely don’t care who you are, where you are,” Levin said. “It is just as easy to send an email to a rural small school as it is to a large bank.”

4. Be Careful With Suspicious-Looking Links

In the days and weeks ahead, Levin said, schools need to redouble their precautions against opening suspicious links and email attachments from unknown or dubious addresses.

“School districts would do well to warn and build awareness, among both students and teachers, to have a little bit of skepticism when they are getting information appearing in their inboxes related to coronavirus, just to double-check who it is being sent from, whether this was an email they were expecting,” Levin said. “If it’s from an email address they don’t recognize or normally don’t get messages from, I think it’s important to double check that email address.”

He added that if teachers or students think they’re receiving phishing emails, they should reach out to their IT staff to report it immediately.

5. Schools That Already Practice Good Cybersecurity Should Be Safe

Levin emphasized that for schools that are already on the lookout for cybercrime, their preventative measures should be enough.

“This is a time when schools would do well to be extra vigilant,” he said. “But the good news is these sorts of incidents [can be prevented] if there are good cybersecurity practices in place already.”

The coronavirus pandemic and the phishing scams that come in its wake should be a reminder, Levin said, that cybersecurity “needs to be a part of schools’ continuity plan.”