STATE OF SOUTH CAROLINA
DEPARTMENT OF EDUCATION

MOLLY M. SPEARMAN
STATE SUPERINTENDENT OF EDUCATION

MEMORANDUM

TO: District Superintendents
Technology Coordinators

FROM: Kenneth B. Puett, CISSP
Chief Information Security Officer

DATE: June 24, 2016

RE: Phishing Email Attacks

In the last several days, a series of "Phishing Emails" has been sent from different sources including Excent Corporation which is a premier vendor of PowerSchool and Enrich IEP.

In Phishing Attacks, typically a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs, or credit card details. Phishing is a homophone of fishing, which involves using lures to catch fish.

Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate email than trying to break through a computer's defenses. Although some phishing emails are poorly written and clearly fake, sophisticated cybercriminals employ the techniques of professional marketers to identify the most effective types of messages – the phishing "hooks" that get the highest "open" or click through rate and the Facebook posts that generate the most likes. Phishing campaigns are often built around the year's major events, holidays and anniversaries, or take advantage of breaking news stories, both true and fictitious.

To make Phishing messages look like they are genuinely from a well-known company, they include logos and other identifying information taken directly from that company's website. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization.

Scam emails and websites also can infect your computer with malware without you even knowing it. The malware can give a criminal access to your device, enabling them to access all your sensitive files or track your keyboard strokes, exposing login information.

Here are a few simple steps you can take to protect yourself:

- Change your password as soon as possible if you have clicked on a link in the email. At this point, they know your login and password.
- Avoid suspicious phishing emails that appear to be from the IRS or other companies; do not click on the links – go directly to their websites instead.
- Beware of phishing scams asking you to update or verify your accounts.
- To avoid malware, don't open attachments in emails unless you know who sent it and what it contains.
- Download and install software only from websites you know and trust.
- Use security software to block pop-up ads, which can contain viruses.
- Ensure your family understands safe online and computer habits.

The South Carolina Department of Education is committed to protecting our students' and teachers' sensitive data by proactively addressing security concerns as well as providing relevant and timely security expertise to our school districts and their technology personnel. Our Chief Information Security Office can offer assistance in a variety of methods and can be reached at (803) 734-8301.

Thank you.

cc: Technology Coordinators