SWWC CYBERSECURITY

Spear Phishing on the Rise as School Year Begins

By Brady Carstens, Cybersecurity Engineer and Josh Sumption, Chief Technology and Information Officer

Another school year is ramping up with all the hustle and excitement that comes with it. With our primary focus on getting ready for another year of educating the future generation, cyber criminals grin at the opportunity to catch us with our guard down on cyber activity. Already in this new school year, SWWC Cybersecurity has observed an uptick in cyber incidents, especially in Spear Phishing attacks against school staff. "Spearfishing?" you might ask. "How is that different from the phishing I have become so familiar with in the past and how exactly will this impact my school district?" Spear Phishing is a form of phishing used by bad cyber actors in attempt to make money. But unlike normal phishing, spear phishing takes things a step further when the bad actor directly calls out a single person or organization with the hope of increasing the number of victims.

SWWC Cybersecurity has identified multiple spear phishing attempts involving someone pretending to be the CEO or Superintendent of Schools sending text messages and emails to employees asking for gift cards, which is a method of attack seen several times over the past couple of years. This summer, however, we have observed the sophistication of these attempts increase dramatically.

One of the latest spear phishing attempts that we have responded to occurred in a school district where staff have been transitioning Email platforms and have had several security awareness reminders and were quite diligent. The attack began on August 12 with an email spoofed to appear as though it was coming from an actual employee of the school district. The threat actor was most likely able to find the employee's name and email address from the school district's staff directory on their website. The email was sent to the district's payroll department stating that they needed to change their direct deposit before the next paycheck. Ok, we know what you are thinking here, this is another one of those classic attempts that we have seen occur in my school a few times in the past. The difference in this spear phishing attempt is that the email included the name of the payroll specialist and the full name of the employee who was trying to change bank account information. Further, to make this attempt even more sophisticated, the department secretary who received the original request was on vacation when the original email was sent, and their out of office reply stated that they would return on August 23. On August 23, the actor once again emailed the payroll specialist using the spoofed name and Email address of the district staff member to verify that the bank information had been changed. This time the threat actor also included the district's required direct deposit form fully filled out with the employee's information and included a voided check that had been edited with the employee's actual name and address. *(Redacted image of the check presented is shown at end of article).*

In this specific incident, the Email, request form and voided check did make it past the payroll department's administrative assistant at the school district, who passed the request on to the

payroll specialist. The payroll specialist was suspicious about the request, and upon communicating over the phone with the employee who appeared to initiate the request, found that the employee had no knowledge of the request. The spear phishing attempt was stopped in its tracks and reported to SWWC's Cybersecurity staff for further review.

We would like to share a couple of insights and lessons that should be learned from this example of spear phishing.

- How did the actor produce a copy of the school district's official direct deposit request form? In a quick review of the school district's website, SWWC Cybersecurity found that the direct deposit, among other payroll and employment forms, were available on a publicly accessible section of the school district's website. It is important to make sure that these types of resources are not publicly available and are only available to those fully authenticated and authorized to access your organization's digital resources. Do not rely on a generic username and password to protect these resources, as those credentials are easily shared and can accidentally fall into the hands of those who will misuse them.

- How did the actor produce a cancelled check for the new account to submit with the direct deposit form? The check presented to the district's staff with the change request form may look convincing at first, but upon careful inspection, one should notice that it is clearly missing the classic check number at the top right corner of the check. Additionally, the bank routing and account numbers are not displayed in a MICR font and are also labeled, both of which do not meet banking industry standards.

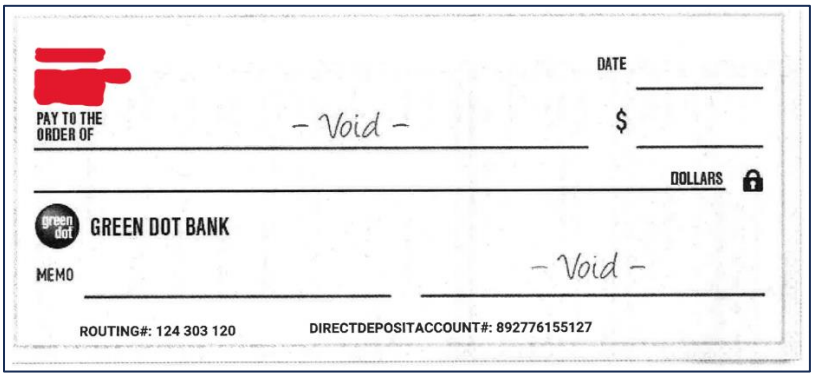
This real-world experience exemplifies the importance of cybersecurity in our everyday lives, especially when our decisions could impact the lives of others. Cybersecurity is just as much about building individual's knowledge and understanding through continuous professional development as it is the technical components and analysis that are managed by cybersecurity experts.

Unfortunately, there is little that can be done to prevent future events like this from happening. The most effective mitigation solution to follow that helps minimize the potential impacts of these types of events is referred to as "least privilege." Least privilege is only giving individuals access to information on a need-to-know basis, nothing more and nothing less. Another preventative measure is to ensure that your employees have proper training when it comes to cybersecurity. Proper training includes, but is not limited to, phishing campaigns, phishing training, password training, and zero trust training. It is also important to remember that cybersecurity awareness trainings are not one-and-done events. They require continuous remediation to keep users up to speed on new threat tactics and refreshed on those we may not have seen in a while.

SWWC CYBERSECURITY

Spear Phishing on the Rise as School Year Begins

If you are interested in training or any of our Cybersecurity services, please reach out to cybersecurity@swwc.org. SWWC Cybersecurity provides a comprehensive catalog of both on-demand and customized in-person training in all areas of cybersecurity at affordable rates. SWWC Cybersecurity also provides cybersecurity as a service so if you or your organization. Visit www.swwc.org/cybersecurity for more information.



(Redacted image of check presented)