June 2018

NCDPI Cybersecurity Newsletter

Welcome to another NCDPI Cybersecurity newsletter in our series of communications. For those seeing this for the first time, my name is KC Hunt and I am the NCDPI's Information Security Officer. This newsletter is dedicated to phishing. DPI as well as districts have seen a serious uptick in the amount of phishing emails targeting our employees. Some successful phishing emails include LEA's compromised with the EMOTET virus. The city of Charlotte compromised with ransomware. The city of Atlanta compromised with ransomware.

10 Tips to determine if the email is phishing:

Phishing has become one of the most pervasive problems facing data security staffs today. A basic phishing attack is relatively easy to conduct and inexpensive for the attacker. When you are going through your email and before you click that link, here are some rules of thumb to consider first:

1. Does the email ask for personal or sensitive information, such as your date of birth, Social Security Number, an account number or login credentials? Most legitimate businesses do not request such data in an email.
2. Does the email ask you to click on a link to access a web site? If so, that site might be fake.
3. Does the email have a generic salutation rather than your name? Your bank or service provider know who you are and normally will address you by name.
4. Does the email have an attachment? If you are not expecting an attachment, don't click on it. Confirm its validity first with the sender using a phone call or text.
5. When you move your mouse over the email, is the entire email is a hyperlink? If so, it likely is a phishing attack.
6. If the email makes an offer too good to be true, such as a large sum of money, a prepaid gift card or an expensive piece of electronics for free, it's likely a phishing attack.
7. Be careful of emails that make an emotional plea while asking for money. While many charities use such tactics, it also is a popular approach used by phishers.
8. If the email claims you have an immediate problem, such as a virus or that you are running out of email storage space, and you must take immediate action, be careful. This is a common phishing tactic.
9. If the email makes a direct threat and requires that you take immediate action by clicking a link for the IRS, a police agency or the like, it's probably fake.
10. An email might appear to be from a friend asking for money. Never send money without calling the friend first to confirm the request.

Charlotte Housing Authority W-2

At the end of January this year, Charlotte Housing Authority was hit with a phishing email scam which lead to the compromise of all current and former employee's W2 records. The housing authority said an email was sent to an employee purportedly from the CEO asking for all current and former W-2 records. The email was received and acted upon, but the fact that it was fraudulent was not discovered until late January. The information compromised includes employee names, addresses, Social Security numbers and wage information. Last year one of our school districts was compromised in a very similar manner. Sensitive information should never be emailed unless other protections are in place i.e. encrypted or password protected. The password should always be communicated to the receipting of the email in an out of band method; phone call, text, in person.

Gmail Phishing Scam of the week

Scam of the Week: Fiendishly Clever Gmail Phishing You Need to Know About

Here is how this scam works. The victim receives a text asking whether they've requested a password reset for their Gmail account - and, if not, to reply with the word 'STOP'.

Employees who have not received any security awareness training could likely fall for this social engineering tactic, and will respond with 'STOP'. Next, they are urged to send the 6 digit numerical code in order to prevent the password being changed.

Of course what is really happening is that the scammer has requested a password change on their account. That request sends a code to the real account owner to verify that they actually want the password changed. And by sending the attacker that code back, you're enabling the bad guys to complete the password change, and now they have access to the account and all the email.

Remember that Gmail or any other web email service will never ask if you *don't* want to do something with your account. You didn't ask for a password reset, so you shouldn't be asked about one.

Do not reply to the text (doing so will tell the scammers that they have reached a valid number). And to prevent losing your account to bad guys, it's a very good idea to have 2-step verification set up on your Google account."

Please feel free to suggest topics that you would like addressed in upcoming newsletters by contacting me at kc.hunt@dpi.nc.gov or (919) 807 4068.

Public Schools of North Carolina
State Board of Education
Department of Public Instruction

Stay Connected with North Carolina Public Schools: