MCX

CMAA
Construction Management
Association of America

Member Communication Experience

The Ongoing Risk of Phishing in the Construction Industry

Written by: Andrew Parks, Managing Security Consultant, FoxPointe Solutions, and Marie Gavin, Manager, The Bonadio Group

The construction industry is continually assessing and adapting technology solutions in order to make better decisions, improve jobsite security, increase productivity, and reduce risk.

Various technology solutions that been implemented within the construction industry workflow include CAD software and drones for surveying environments deemed too difficult or dangerous for personnel. Various future state technologies being adapted include artificial intelligence, which can sort through data faster than humans for useful insights and trends, and virtual representation of buildings for testing projects against the conditions of nature, such as high winds or floods prior to construction.

It's important to note that with the adoption of technology, there has not been an equivalent in training and proper use of these added solutions. This lack of training increases an organization's vulnerability to hackers. Additionally, these technologies can be integrated in systems where passcodes are not changed regularly and access is not limited to certain individuals.

With this increased reliance on technology comes the inevitable attention of malicious third-party actors such as cybercriminal groups and nation state hacking groups who seek to gain, for financial or political reasons, information and data meant to remain private to the company. According to Verizon's 2021 Data Breach Investigation Report, the most common data breach within the construction industry is web application attacks, which are facilitated by stolen credentials, with the majority of stolen credentials being obtained by social engineering attacks such as phishing.

THE TRUE COST OF A DATA BREACH

Some contractors may have the perception that cyberattacks will not happen to them as they are not a large enough company to gain any attention from hackers. There may also be a misconception of how valuable data such as bid information, design information, materials pricing, proprietary assets, profit and loss data, confidential employee information, and company banking records is. Each of these items can be used to target specific companies for phishing data breaches. Furthermore, smaller construction companies are small may not have the financial resources for an IT department, creating additional vulnerabilities as financial resources are not used to update equipment, invest in software to limit malicious attempts on the company's system, and/or cyber insurance. But if a data breach does occur, what is the true cost?

A recent Forrester survey stated that more than 75% of respondents in the construction, engineering, and infrastructure industries had experienced a cyber-incident within the last 12 months. Costing businesses approximately $6 trillion per year on average through 2021.

While traditional mass email phishing attempts are still very efficient, cyber criminals have adapted and are expanding their phishing efforts to other medias such as texting, known as "smishing," and voice calls, aka "vishing," in addition to traditional emails. While these malicious third parties continue to adapt, te construction industry must also modify its defense structure to look past traditional anti-phishing technologies such as email spam filters and implement controls appropriate for the evolving risk these malicious groups pose.

According to Verizon's 2021 Data Breach Investigation Report, internal threats within the construction industry remain low at about 5%, with external threats around 95%. However, at 4.5% the click rates of malicious links within phishing emails for the construction industry was found to be 1% higher than the average of all other industries. This shows that the construction industry is especially vulnerable to these types of attacks.

IBM shows that the average cost of a data breach is approximately $4 million, meaning companies should not only be aware of phishing risks, they should also be preparing with various security controls aimed to mitigate the possibility of these attacks.

INCREASED RISK DURING THE COVID-19 PANDEMIC

Additionally, the COVID-19 pandemic introduced the added opportunity for malicious actors to exploit vulnerable people and organizations through targeting government assistance programs. According to KnowBe4, 50% of phishing attacks attempted in Q3 2020 referenced either stimulus checks or the Paycheck Protection Program loans in the subject line. Unfortunately, by playing off the uncertainty of the pandemic and the immediate need of funding for many companies, attackers were extremely effective during 2020.

ADDRESSING THE RISKS

There are multiple controls that management can implement to limit the risk of phishing attacks against their employees and environment, including email spam filters and employee education.

Email spam filters can detect and block well-known scamming emails and contents. However, it's important to note that new phishing emails can and will get past the best email spam filter and employee education is essential in identifying these and alerting IT. Employees should be trained on a regular basis to be able to identify phishing attempts. Training should include guidance for recognizing emails, such as evaluating email addresses, identifying any misspellings in the email, ensuring all links are legitimate and known prior to clicking on them and spotting problematic language. For example, phishing emails often contain language such as "I need your help," and or "please provide your personal information."

There are various types of controls aimed to limit credentials being comprised, including Multi-Factor Authentication, instituting a 90-to-120-day rotation of passwords and using proper access controls. MFA can ensure that the compromise of the user ID and password will not be sufficient in order to gain access to the systems. Instead, the malicious individual would also have to compromise a second factor, which could include additional questions or may send a confirmation code to the user's email or phone.

Other suggestions include knowing who the company's third-party vendors use for IT security, especially the vendors that are used for the compiling of W2s and other tax forms.

Proper access controls are also essential in limiting the risk to the enterprise for a compromised account. If this occurs, accounts should be locked down to only the system and data they need to perform their job duties and no more.

BE DILIGENT AND STAY INFORMED

While phishing and other cybersecurity attacks aren't completely unavoidable due to the heavy amounts of technology used today, there are several ways that construction companies can protect themselves from these scams. Staying aware and diligent when analyzing threats by putting in place the proper security measures and training employees can not only help to safeguard employee and company information, but also save the company millions in damages.

About the Authors

Marie Gavin is a Manager at The Bonadio Group.

Andrew Parks is a Managing Security Consultant at FoxPointe Solutions. He can be contacted at APArks@FoxpointeSolutions.com.

About the Article

Republished from Construction Executive, a publication of Associated Builders and Contractors. Copyright 2021. All rights reserved. Associated Builders and Contractors is a national construction industry trade association representing more than 21,000 members. Based on the merit shop philosophy, ABC helps its members develop people, win work, and deliver work safely, ethically, and profitably for the betterment of the communities in which they work.

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.