PARKER SMITH & FEEK
An IMA Company

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

GENERAL INFORMATION

NOVEMBER 3, 2021

Breaking Down Cybersecurity Measures

Alex Adams | Elite Account Executive

In today's ever-evolving cyber environment, hackers have become intrusion specialists with increasingly sophisticated ways of compromising your system's integrity. Using social engineering and ransomware attacks, these bad actors have generated millions in revenue through Bitcoin ransom payments and tricking victims into voluntarily transferring funds.

The days of hackers going after personal information are not gone, but they have found quicker ways to monetize their efforts. They can get paid faster if they hold a company's system hostage for a Bitcoin ransom or trick someone into voluntarily transferring tens of thousands of dollars to them directly with social engineering.

In response to the increase in these attacks, cyber insurance carriers have reacted in several ways, most commonly by requiring companies to implement multi-factor authentication and strict call-back verification procedures to provide cyber coverage. There is a good reason for these requirements - they are extremely effective when implemented correctly.

UNDERSTANDING COMMON CYBERSECURITY TERMS

When talking about cyberattacks, it is important to understand the following terms: social engineering, ransomware, call-back procedure, and multi-factor authentication.

Social Engineering

The art of manipulating people in an online environment, encouraging them to divulge, in good faith, sensitive information, such as account numbers, passwords, or banking information. Social engineering can also take the form of the "engineer" requesting the wire transfer of monies to what the victim believes is a

ABOUT PARKER, SMITH & FEEK

Parker, Smith & Feek is a private brokerage firm driven by client service. We offer a range of services, including commercial insurance, risk management, surety, employee benefits, and personal insurance. PS&F is ranked nationally as one of the 40 largest privately held risk management and insurance brokers. We are committed to serving the community and proud to be one of the top corporate philanthropists in the region.

LEARN MORE

About Parker, Smith & Feek
Industry Overview
Our Services

CONTACT US

Email
Tel: 800.457.0220

FOLLOW US

continued >

financial institution or person, with whom the victim has a business relationship, only to later learn that the funds have landed in the account of the "engineer."

Ransomware

A type of cyberattack that blocks access to a victim's data, website, client services systems, or other critical resources. The ransomware is then used to demand payment in return for unblocking access to the victim's resources.

Call-back Procedure

A conversation with the third party purporting to be an employee, client, customer, vendor, or business affiliate to verify their identity and request's authenticity.

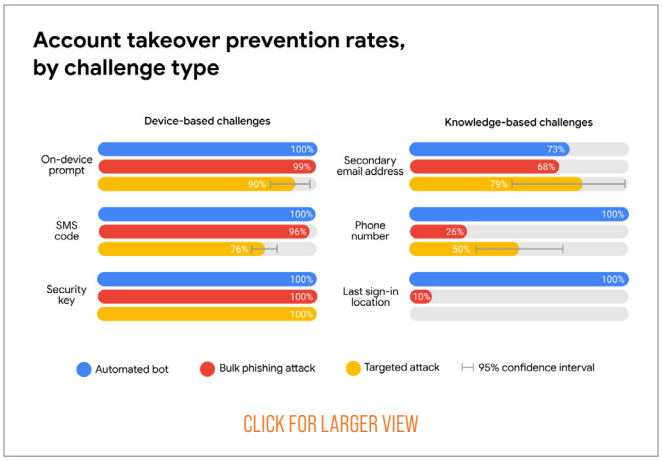
Multi-factor Authentication (MFA)

A process that strengthens access security by requiring two or more factors to verify a user's identity. These factors can include something you know (username and password) plus something you have (smartphone) to approve authentication requests. Most of us are familiar with the process of getting a code texted to your phone to log into banking and other applications.

MULTI-FACTOR AUTHENTICATION

Let's dive into what various types of MFAs are available. The two main groups we will explore are device-based verification (i.e., challenges) and knowledge-based challenges. Device-based challenges include on-device prompts through programs downloaded onto a personal device (most commonly a mobile phone), an SMS message sent with a code directly to the user's mobile phone, or a physical security key kept by the user. Knowledge-based challenges verify a user's identity by asking them to confirm an email address, phone number, or last sign-in location.

In 2019, Google partnered with New York University to fund a study to investigate prevention rates for each of the three most common hacking methods:



CLICK FOR LARGER VIEW

With numbers like these, it is not hard to understand why insurance companies prefer to insure businesses that take these steps to protect themselves. While there is some debate about the study's methods, these are the most comprehensive studies completed to date. Security keys are by far the most effective, but they require employees to carry a physical key, which is why the on-device prompt is currently the most popular of these methods.

One of the other most common methods of tricking companies out of their hard-earned money is social engineering.

Social engineering has many different forms and may involve a breach of your system, but that is not required for the most common method called "phishing," which often involves spoofing or duplicating a legitimate email to trick your employees into divulging sensitive information. It is often extremely difficult to tell a fake email from an authentic one, and when hackers are only adding or shifting letters around, it can slip by unnoticed. Further, if hackers do breach your system, they can often wait for months observing email traffic, looking for the perfect moment or client relationship to exploit. Once identified, they can either email your clients/vendors asking them to change incoming payment information or pose as a vendor asking your company to change

continued >

outgoing payment information. Luckily, these can both be thwarted by implementing a strict call-back procedure not just with your staff, but your contracts and invoices as well.

CYBERSECURITY PREVENTION BENEFITS

These safeguards and processes can not only save your company money and time by preventing these sorts of direct attacks, but they can drastically affect the cost of your cyber insurance. Some companies must pay four times more premium because they do not have these protections in place. Further, some carriers will not provide cyber coverage at all to companies without some form of prevention measures.

The last thing to consider is how user-friendly a given system is for your workforce. This same study done by the New York University looked at the success rate of multi-factor authentication systems using an on-device prompt. It found that 88.2% of users could gain access to their accounts immediately and that 98.4% figured out the two-factor system within one week. Which such a high success rate, it's not hard to understand why this is often the method of choice.

Your insurance broker should be able to assist you with finding a reputable MFA provider or develop your call-back procedures to help drive down your cyber insurance premiums. If you have questions or would like to learn more, reach out to Parker Smith & Feek, and we will be more than happy to discuss these and any other risk management questions you may have.

References and Resources

1. Social Engineering, International Risk Management Institute, Inc. (IRMI). https://www.irmi.com/term/insurance-definitions/social-engineering
2. Ransomware, International Risk Management Institute, Inc. (IRMI). https://www.irmi.com/term/insurance-definitions/ransomware
3. Call-back Verification Procedure, Law Insider Inc. https://www.lawinsider.com/dictionary/call-back-verification-procedure#:~:text=Call%2Dback%20Verification%20Procedure%20means,communication%20from%20such%20Third%20Party
4. Multi-Factor Authentication (MFA), National Institute of Standards and Technology (NIST). https://csrc.nist.gov/glossary/term/multi_factor_authentication
5. Google Data Explain the Importance of Setting up a Recovery Number to Prevent Phishing Attacks, Techweez. https://techweez.com/2019/05/20/google-advanced-security-2fa-phishing-data/
6. Doergler, Marincenko, Ranieri, Jiang, Moscicki, McCoy Thomas 2019 Evaluating Login Challenges as Defense Against Account Takeover New York University Google Study. https://research.google/pubs/pub48119/