MULTIFACTOR AUTHENTICATION

AN IMPERATIVE FOR VOTER RECORD SECURITY
IN THE ERA OF CYBERSECURITY THREATS

A GCR COMPANY

Hank is easily the most dedicated volunteer in the county elections office. He possesses institutional knowledge, knows how to properly set up an election, and is trusted by the elections officials to train other volunteers. Hank has a password and is given access to the voter database to enter changes to voter records during busy times in the election cycle. While it took awhile to learn, he now can log in to the system, make basic voter information changes, and log out. Hank also has access to email on the system, in order to receive occasional updates and bulletins from the Secretary of State.

One day, Hank is logged in to the voter database performing some voter file updates when he is alerted to a new email just received. He clicks on the email alert and is linked to his official email account. Hank opens the new email message, which appears to be notification that his email account must be updated in order to continue receiving emails. Hank is expecting an important bulletin from the Secretary of State about the upcoming election, and he does not want to miss it. He dutifully clicks on the link in the email that includes the web browser logo and looks very legitimate. Once on the linked page, he is prompted to provide his email account and password information. He thinks twice about giving up his password, but then remembers how the previous link appeared so official, using the trademarked logo of his browser. He enters his credentials. The screen goes blank for a moment, then kicks out of the account update site. He shakes his head, perplexed, then goes back to completing his work updating voter records.

Twelve weeks later, it is determined during the general election that a significant number of voter records have been deleted or amended in Hank's county, and voters are left to cast provisional ballots at the polls. The changes impact only registered members of one political party and the election produces an unexpected result.

THE PROBLEM

Automated systems leverage technology to promote efficiency and to process volumes of data accurately. Such technology is essential to the operation of elections on a scale necessary in a modern democracy. But bad actors persist in any system, and the bad guys have access to technology, as well. According to the US Department of Homeland Security (DHS), there were attempted intrusions into elections systems throughout the United States in the 2016 Presidential Election cycle. In its Security Tip ST16-001 (released September 15, 2016), DHS notes, "Voter registration databases and election systems are rich targets and may continue to experience frequent attempted intrusions."[i]

Modern voter registration and election management systems are susceptible to malicious activities and must be designed and monitored to fend off cybersecurity threats. "Malicious actors may use a variety of methods to interfere with voter registration websites and databases."[ii] One insidious and prolific risk is the phishing attack, which uses social engineering to trick victims into providing their login credentials to an otherwise secure system.

"Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable… company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts."[iii] "Phishing emails attempt to manipulate users into clicking on a malicious link or downloading a malicious file attachment.

SYSTEMS INFECTED THROUGH PHISHING ATTACKS ACT AS AN ENTRY POINT FOR THREAT ACTORS TO SPREAD THROUGHOUT AN ORGANIZATION, STEAL VOTER INFORMATION, OR DISRUPT VOTING OPERATIONS."[IV]

"Attackers often take advantage of current events and certain times of the year, such as major political elections."[v]

Voter registration and election systems are particularly susceptible to phishing attacks because such systems rely on large numbers of peripheral users to enter data. Peripheral users are trained in how to use specific systems but may vary in levels of general computing sophistication. The fictitious account that introduces this paper illustrates how the most trustworthy and experienced election worker could unwittingly expose state and voter data by falling victim to a phishing scam. Even relatively savvy computer users can be fooled by ever more sophisticated scams with compelling designs. Bad actors incorporate real logos, state seals, and other indicia lifted from legitimate sites to ply their illicit trade. The rising sophistication of phishing attacks creates an ever-increasing risk of exposure.

HOW PHISHING ATTACKS WORK: DIGITAL IMPERSONATION

The National Institute of Standards and Technology (NIST) explains how phishing attacks work. Such attacks are predicated on digital impersonation. According to the NIST:

> *Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to be traceable back to a specific real-life subject. In other words, accessing a digital service may not mean that the underlying subject's real-life representation is known…Digital identity presents a technical challenge because it often involves the proofing of individuals over an open network and always involves the authentication of individuals over an open network. This presents multiple opportunities for impersonation and other attacks which can lead to fraudulent claims of a subject's digital identity.*[vi]

In other words, anyone who possesses the network and or application credentials of another can impersonate the access-privileged person and gain access to their network. In a phishing attack, the bad actor utilizes social engineering tricks to elicit the credentials of a subject. Once those credentials are known, the bad actor hacks into the application undetected, standing in the shoes of a legitimate user.

FIGHTING THE ROOT CAUSE OF PHISHING ATTACKS: DIGITAL AUTHENTICATION

Phishing attacks are predicated on the misappropriation of an application user's access credentials, allowing the bad actor to impersonate a legitimate user. It stands to reason, therefore, that the most direct means of preventing a phishing attack is to bolster and protect digital identity. This can be accomplished through digital identity authentication, as noted by NIST in the same publication:

> *Identity proofing establishes that a subject is actually who they claim to be. Digital authentication is the process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as the one who accessed the service previously.*[vii]

"Authentication is performed by verifying that the claimant controls one or more authenticators (called tokens in earlier versions of SP 800-63) associated with a given subscriber. A successful authentication results in the assertion of an identifier… and optionally other identity information."[viii] When additional identity elements are added to the authentication protocol, two-factor or multifactor authentication is achieved. It stands to reason that adding more authentication factors (identity requirements) can bolster network security against identity-based intrusions such as phishing attacks.

LIMITING RISK THROUGH APPLICATION OF BEST PRACTICES: MULTIFACTOR AUTHENTICATION UTILIZING OUT-OF-BAND AUTHENTICATORS

In years past, it was deemed sufficient to protect an application by requiring a User Name and Password combination. Over time, sneaky criminals have found ways to elicit such combinations from unwary users. As a result, authentication protocol is more important now than ever before. Moreover, the strongest password protocols are not even safe from intrusion. Over time, technology has developed to thwart the bad actors. Criminals rely on the anonymity of the authenticating individual inherent in traditional authentication schemes. The only effective way to defeat a phishing attack is to change the security approach. Creating an additional authentication protocol that requires a physical element virtually blocks the bad actor's access to the application.

The Center for Internet Security (CIS) is a reputable nonprofit organization that sponsors the MS-ISAC (Multi-State Information Sharing & Analysis Center) infrastructure security initiative. CIS has done much to advocate for secure elections infrastructure and published in February 2018 its Handbook for Elections Infrastructure Security (CIS Handbook), disseminated at the Winter 2018 meeting of the National Association of Secretaries of State (NASS). The Handbook includes an extensive set of Best Practices.

TABLE 1, below, is an abstract from the CIS Handbook, and points to the importance of employing multifactor authentication to harden voter registration and election management infrastructure against phishing attacks:

TABLE 1: *Best Practices to Protect Data and Systems from Phishing Attacks*
From A Handbook for Elections Infrastructure Security, Center For Internet Security (February 15, 2018)

Require the use of multi-factor authentication

Applicable CIS Controls

#5.6: Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

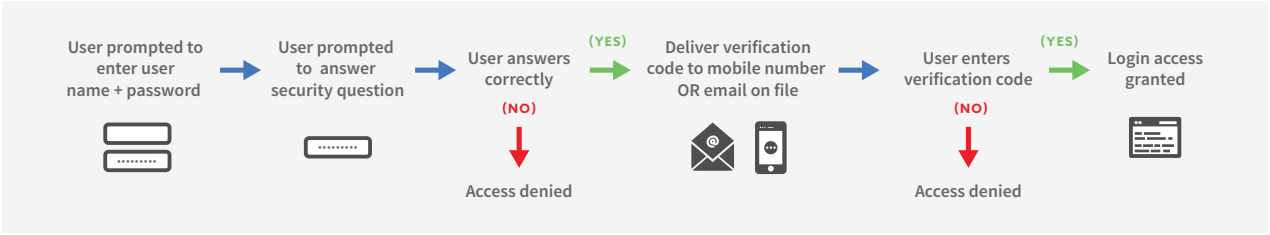
#12.6: Require Two-factor Authentication For Remote Login
Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

#16.11: Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	High	Medium

Resources
Vendor specific. NIST guidance on authentication: https://pages.nist.gov/800-63-3/sp800-63b.html.

MOBILE | EMAIL AUTHENTICATION



Because any digital identifier is capable of exposure, the best kind of multifactor authentication requires a physical exchange outside the digital realm. The NIST refers to such an identifier as an "out-of-band authenticator."[ix]

One such out-of-band authenticator is when "The claimant transfers a secret received by the out-of-band device via the secondary channel to the verifier using the primary channel. For example, the claimant may receive the secret on their mobile device and type it (typically a 6-digit code) into their authentication session."[x]

BY EMPLOYING AN OUT-OF-BAND AUTHENTICATION ELEMENT AS PART OF THEIR MULTIFACTOR AUTHENTICATION PROTOCOLS, ELECTION OFFICIALS CAN VIRTUALLY ENSURE THAT A PURLOINED PASSWORD WILL NOT BECOME A DATA BREACH THAT COMPROMISES AN ELECTION.

CONCLUSION

Secretaries of State, Election Commissioners, Election Directors, and Information Officers are at the point, perpetuating democracy by protecting voter information and elections. It is critical to coordinate with a knowledgeable vendor to make multifactor authentication a crucial part of your system's defenses against cybercrime.

PCC Technology Inc., sponsor of this white paper and longtime sponsor of NASS, is proud of its record of defending democracy by implementing security-focused voter registration and election management systems for over two decades.

READY TO INNOVATE?

Call now for a demo or for additional info:

860.242.3299

PCCtechnologyinc.com

This white paper was prepared by PCC Technology Inc., a leading national provider of state and municipal market government sector software. Our aim is to develop, implement and support advanced automation solutions that assist agencies to administer their business with maximum efficiency, while driving unprecedented levels of transparency and public access to data. PCC Technology Inc. is experienced in working with state clients to design, implement, and maintain secure voter registration and election management systems across the country. For additional information, contact Sales Executive **Seth Klaskin** at (**860)580-7301** or **seth.klaskin@pcctg.com.**

[i] *Security Tip ST16-001 Securing Voter registration Data*, US Department of Homeland Security (September 15, 2016).
[ii] *id.*

[iii] *Security Tip ST4-014 Avoiding Social Engineering and Phishing Attacks*, United States Computer Emergency Readiness Team (US-CERT), US Department of Homeland Security (October 22, 2009).

[iv] *Security Tip ST16-001 Securing Voter registration Data*, US Department of Homeland Security (September 15, 2016).

[v] *Security Tip ST4-014 Avoiding Social Engineering and Phishing Attacks*, United States Computer Emergency Readiness Team (US-CERT), US Department of Homeland Security (October 22, 2009).

[vi] *NIST Special Publication 800-63B Digital Identity Guidelines: Authentication and Lifecycle Management*, National Institute of Standards and Technology, US Department of Commerce (June 2017)
[vii] *id.*
[viii] *id.*
[ix] *id.*
[x] *id.*