Security of Election Announcements

TABLE OF CONTENTS

SECURITY OF ELECTION ANNOUNCEMENTS

ISSUE

How secure from cyber attacks is the online election information San Mateo County provides to the public?

EXECUTIVE SUMMARY

Much of the public attention on the topic of election security focuses on the integrity of voter registration databases, voting machines, and vote tabulation. This report is not about the integrity of individual votes. Instead, this report focuses on the vulnerabilities of the County's email and online communication platforms to hijacking and propagating disinformation in the guise of election instructions or announcements.

Illustrating the Threat

Imagine that a hacker hijacks one of the County's official social media accounts and uses it to report false results on election night and that local news outlets then redistribute those fraudulent election results to the public. Such a scenario could cause great confusion and erode public confidence in our elections, even if the vote itself is actually secure. Alternatively, imagine that a hacker hijacks the County's elections website before an election and circulates false voting instructions designed to frustrate the efforts of some voters to participate in the election. In that case, the interference could affect the election outcome, or at least call the results into question.

ACRE's Use of Online Systems to Deliver Election Information

The U.S. Department of Homeland Security (DHS) encourages voters to get election information directly from their local elections office. In San Mateo County, the office of the Assessor-County Clerk-Recorder and Elections (ACRE) is responsible for carrying out elections and announcing local results. ACRE uses the following online communication platforms to disseminate election information to the public:

(1) Email: ACRE sends election information via email to approximately 43,700 registered voters who previously signed up to receive electronic-only delivery of sample ballots and voter information. The County's Information Services Department (ISD) manages County employee email.

(2) Website: ACRE uses the smcacre.org website to publish voter eligibility information along with instructions on how to register to vote, the locations of vote centers, voter instructions, and official local election results for ballots cast within the county. ACRE asked ISD for a limited review during the procurement of the website hosting services,

but ISD is available to all departments for extensive website procurement support and is even able to host department websites itself.

(3) Social Media: ACRE uses its own official Twitter, Instagram, and YouTube accounts to share election information. ACRE also enlists the County Manager's Office (CMO) to help disseminate election information through the CMO's official Facebook and Nextdoor accounts.

Concerns about the security of these communications channels are not theoretical. In 2010, hackers hijacked ACRE's election results webpage and, in 2016, cyberthieves successfully breached several County employee email accounts using "spear phishing" techniques.

The County's Current Security Methods

In the wake of the spear phishing attack on County email accounts and in an effort to prevent future email account takeovers, the County put in place a multi-factor authentication system that requires users to enter more than just a single password when they log in. This system requires that employees logging in to their email must, in addition to their password, supply extra information that is supposed to be difficult for cyber criminals to obtain. The additional information that many County employees now enter as part of the login process is a unique, one-time authentication code they receive contemporaneously as a text message on their cell phones. CMO uses a similar multi-factor authentication system to prevent a hacker from taking over its official Facebook page. However, there is no multi-factor authentication protection for any of the other social media accounts used by ACRE to broadcast election information or for logging in to ACRE's website to make changes to it. Additionally, although ISD has a policy against email account password sharing because of the security risks associated with the practice, CMO encourages County departments to share the passwords of official social media accounts in case the person normally responsible for publishing messages is unavailable at the time a department needs to post a statement.

Expert Advice on Protection Against Hacking

The theft of online login account credentials is increasingly common, particularly following the development of automated tools that deceive people into sharing their login information on counterfeit websites that appear to be legitimate. The recent publication of these automated tools now allow hackers to more easily compromise accounts protected with the common forms of multi-factor authentication, like the one-time text-messaged access codes that many County employees receive on their cell phones. According to experts, FIDO physical security keys are the only form of multi-factor authentication that always prevents account hijacking. A FIDO key is a small hardware item about the size of a house key that owners can carry on their keychain and insert or tap to their computers or phones in order to complete their account sign-in process.

In addition, according to DHS, an organization can provide an extra layer of protection against efforts to hack email systems by implementing an email verification setting called DMARC. Lastly, organizations can avoid sharing passwords to their official social media accounts by

using an existing feature that allows their employees to use their individual work accounts to manage their organizations' accounts.

Free Resources Available To ACRE

There are eight free cybersecurity services that DHS tailors to local elections offices and offers upon request (see Table 2 in Discussion). Some of these DHS services directly relate to the type of risk this report details—namely that of hackers taking over an online communication account. However, ACRE has not taken advantage of many of these free DHS services.

Conclusions

The Grand Jury finds that the security protections against hijacking of ACRE's website, email, and social media accounts are not adequate to protect against the current cyber threats. These vulnerabilities expose the public to potential disinformation by hackers who could hijack an ACRE online communication platform to mislead voters before an election or sow confusion afterward. Public confidence is at stake, even if the vote itself is secure.

Recommendations

The Grand Jury makes detailed recommendations, which represent short-term fixes to address the immediate risk to upcoming elections and longer-term changes to continually assess the broader cybersecurity threats to election information. In the short term, those ACRE, CMO, and ISD employees critical to the dissemination of election information should protect their accounts with FIDO physical security keys as part of a stronger multi-factor authentication process. In the long term, ACRE and ISD should form a multi-department elections security team in order to evaluate and subscribe to free and tailored DHS services exclusively offered to elections divisions. All of these actions would better safeguard our elections.[1]

[1] This report contains a large volume of technical information, which the Grand Jury intends to serve as a fully-referenced guide for improvements to the security of election announcements. The Grand Jury worded the executive summary for readers less interested in the underlying technology.

AGENCIES

ACRE:
the office of the Assessor-County Clerk-Recorder and Elections in San Mateo County, which is responsible for carrying out elections in the County and reporting local election results, among other things

CMO:
the County Manager's Office in San Mateo County

Controller's Office:
the Controller's Office in San Mateo County performs internal audits of departments' operations, among other things

DHS:
the U.S. Department of Homeland Security

ISD:
the Information Services Department in San Mateo County, which is responsible for managing all County email accounts and the security of the County network, among other things

GLOSSARY

Domain-based Message Authentication, Reporting, and Conformance (DMARC):
a free email setting that reduces *phishing* by eliminating *spoofing*

Fast IDentity Online (FIDO) Alliance:
representatives of technology companies that coalesced to improve account security standards

FIDO security key:
the generic technology for a resilient piece of hardware that owners can carry on their keychain and insert or tap to their computers or phones as part of the account sign-in process

island hopping:
technique used in half of cyber attacks where a hacker penetrates the weaker security of an organization with whom the ultimate target does business in order to more easily breach the security of the ultimate target

man-in-the-middle phishing attacks:
when a convincing counterfeit website acts as a passthrough to *phish* user login credentials and simultaneously authenticate those stolen credentials with the genuine service

multi-factor authentication (often two-factor authentication):
proof of identity at login using the combination of more than one thing the user knows (e.g., password), has (e.g., cell phone or a FIDO physical security key), or is (e.g., fingerprint)

multi-user administration:
a configuration where two or more employees can each control an official County social media page with their own unique accounts, eliminating the need to share passwords

one-time pin or one-time password (OTP):
numeric access codes generated during the multi-factor authentication process that people often receive on their phones

online communication platform:
shorthand in this report for email, the ACRE website, and County social media pages

phishing:
the use of social engineering methods to manipulate unsuspecting people to take an action on behalf of the exploiter, commonly this action is to share login credentials

spear phishing:
targeted and personalized *phishing*

spoofing:
a technique where an attacker impersonates someone else, commonly by falsifying the from header in email to misrepresent belonging to the same organization as the recipient or a trusted third-party organization

subscriber identity module (SIM) hijacking or SIM swapping:
impersonating account holders and deceiving cellular carrier customer service representatives to redirect a number's service to a different phone in the criminal's control

BACKGROUND

Election Threats

Cyber attacks and election interference are two of the top threats in the U.S. intelligence community's[2] "2019 Worldwide Threat Assessment."[3] The 2016 presidential election increased the general public's awareness of threats to the integrity of our democracy, so much so that in January 2017 the U.S. Department of Homeland Security (DHS) elevated the importance of elections systems by deeming them part of the "national critical infrastructure"[4,5]—i.e., "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[6]

When characterizing perceived threats to elections, the press often focuses on the risk of corruption of voter registration files,[7] corruption of vote tabulation,[8] and other unlawful, fraudulent acts.[9] In San Mateo County, the Grand Jury found no reports of voter registration file corruption[10] or credible complaints of invalid vote tabulation.[11,12] Furthermore, the Grand Jury found that there are safeguards in place for these two potential threats:

- a registered voter whose name is illegally removed from the registered voter rolls by hackers can complete same-day registration at voting centers, mitigating the threat of registration removal,

---

[2] Seventeen member organizations work together to form the Intelligence Community including the Central Intelligence Agency, the Federal Bureau of Investigation, and the Department of Homeland Security. See: https://www.intelligence.gov/how-the-ic-works#our-organizations

[3] Coats, Daniel R. "Worldwide Threat Assessment of the US Intelligence Community." Washington, DC: Senate Select Committee on Intelligence, January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[4] Johnson, Jeh. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." *Department of Homeland Security*, January 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[5] "Starting Point: U.S. Election Systems as Critical Infrastructure." *U.S. Election Assistance Commission*. Washington, DC, June 2017. https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

[6] §1016(e) (42 USC §5195c(e)) "United and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001." 2001. 107th Congress. https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

[7] Newman, Lily Hay. "Citing No Evidence, Brian Kemp Accuses Georgia Democrats of Hacking." *WIRED*, November 4, 2018. https://www.wired.com/story/brian-kemp-georgia-democrats-hacking-claim/.

[8] Zetter, Kim. 2018. "The Crisis of Election Security." *The New York Times Magazine*, September 26, 2018. https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

[9] Gardner, Amy. "N.C. Board Declares a New Election in Contested House Race after the Gop Candidate Admitted He Was Mistaken in His Testimony." *The Washington Post*, February 21, 2019. https://www.washingtonpost.com/politics/candidate-says-new-congressional-election-warranted-in-north-carolina/2019/02/21/acae4482-35e0-11e9-854a-7a14d7fec96a_story.html.

[10] There were reports of voter registration leaks in Illinois. See: Wildermuth, John. "Could Russia Hack California's Elections? It Would Be Hard, But Not Impossible." *San Francisco Chronicle*, July 25, 2018. https://www.sfchronicle.com/news/article/Could-Russia-hack-California-s-elections-It-13100934.php.

[11] Grand Jury interviews of multiple ACRE officials.

[12] Marinucci, Carla. "GOP Cries Foul after California Thumping." *Politico*, November 29, 2018. https://www.politico.com/story/2018/11/29/california-2018-midterm-elections-results-voting-republicans-1031072.

- someone whose name is fraudulently added to the voter registration lists by hackers must still show proof of voter eligibility in person when casting a ballot for the first time, mitigating the threat of new fictitious registrations, and
- a registered voter in the county can check the status of his or her ballot online to see when it is received and counted (or if there is a problem counting that particular ballot, e.g., a mismatched signature, that requires followup),[13] mitigating the threat of ballot destruction.[14]

However, the Grand Jury learned of multiple cyber crimes perpetrated against the County that illustrate the concern of protecting the integrity of County election information including (1) a 2010 takeover of the election results webpage[15,16] and (2) a 2016 phishing attack of email accounts of employees in various County departments.[17,18] While none of these attacks appeared politically motivated, DHS notes there are threats of disinformation around elections that have the potential to sow discord and undermine trust in the political process.[19,20] As one former DHS official put it, "can you imagine a rumor that the [Associated Press] has been hacked and all the numbers are off?"[21]

[13] See: https://www/smcacre.org/my-election-info
[14] Grand Jury interviews of multiple ACRE officials.
[15] The Office of Assessor-County Clerk-Recorder and Elections (ACRE) manages a website, smcacre.org, which hosts several sensitive election-related pages including:
(1) smcacre.org/elections for general election information,
(2) smcacre.org/how-vote for detailed voting instructions,
(3) smcacre.org/current-election for important dates, ballot measure information, and more about the current or most recent election,
(4) apps.smcacre.org/raceTRACKER/ to explore the results of votes counted in San Mateo County,
(5) smcacre.org/post/november-6-2018-election-results-0 (and similar pages) for other copies of official election results of votes counted in San Mateo County, and
(6) smcacre.org/my-election-info to look up a particular voter's registration status and the status of a particular ballot cast by that voter.
[16] Grand Jury interview of a County official.
[17] This report does not disclose details of the phishing attack to protect an ongoing FBI investigation.
[18] Grand Jury interview of a County official.
[19] Nielsen, Kirstjen, Jeff Sessions, Dan Coats, and Christopher Wray. "Joint Statement on Election Day Preparations," November 5, 2018. https://www.dhs.gov/news/2018/11/05/joint-statement-election-day-preparations.
[20] "Nielsen Says US Ready for Cybersecurity Trouble." 2018. United States: Associated Press. https://www.youtube.com/watch?v=UneZJ1rNxH4.
[21] Camp, Joseph. "How Secure Are the Midterm Elections?" United States: PBS NewsHour, 2018. https://www.youtube.com/watch?v=r6UQuz5tVV0.

Political Cyber Attacks

The U.S. Department of Justice indictments[22] and Special Counsel report[23] that describe extensive Russian state-sponsored attacks intended to sow discord in the 2016 election continue to drive the news. During the attacks, the Russians gained access to two county elections systems in Florida by using phishing emails.[24] Other recent political cyber attacks include the violation of a Knox County (Tennessee) election results webpage,[25] a phishing attack against the Contra Costa County elections office,[26] the targeting of politicians[27] and related organizations,[28,29] and the hijacking of a corporate social media account to broadcast anti-Israeli messages.[30] Relatedly, the use of politically motivated cyber fraud—often with social media accounts—is a well-known tactic by many different perpetrators who undermined protesters and activists in Tibet,[31] Egypt, and the Philippines, discredited the anti-Russian Ukrainian government, and incited violence against religious minorities in Myanmar.[32,33]

---

[22] Mueller, Robert S., III. "United States of America v. Viktor Borisovich Netyksho et Al." United States District Court for the District of Columbia, July 13, 2018. https://www.justice.gov/file/1080281/download.
[23] Mueller, Robert S., III. "Report on the Investigation into Russian Interference in the 2016 Presidential Election." Washington, DC, April 18, 2019. https://www.justice.gov/storage/report.pdf.
[24] Parks, Miles. "Florida Governor Says Russian Hackers Breached 2 Counties In 2016." *NPR*, May 14, 2019. https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016.
[25] Wofford, Benjamin. "The Hacking Threat to the Midterms Is Huge. And Technology Won't Protect Us." *Vox*, October 25, 2018. https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting.
[26] "Cyber Attack At Contra Costa Elections Department Started With An Email." *KPIX 5 - CBS San Francisco*, March 25, 2019. https://sanfrancisco.cbslocal.com/2019/03/25/cyber-attack-at-contra-costa-elections-department-started-with-an-email/.
[27] Watkins, Eli. "Claire McCaskill Says Attempted Russia Hacking on Her Office 'Not Successful.'" *CNN*, July 27, 2018. https://www.cnn.com/2018/07/26/politics/claire-mccaskill-phishing/index.html.
[28] Dwoskin, Elizabeth, and Craig Timberg. "Microsoft Says It Has Found a Russian Operation Targeting U.S. Political Institutions." *The Washington Post*, August 21, 2018. https://www.washingtonpost.com/business/economy/microsoft-says-it-has-found-a-russian-operation-targeting-us-political-institutions/2018/08/20/52273e14-a4d2-11e8-97ce-cc9042272f07_story.html.
[29] Isenstadt, Alex, and John Bresnahan. "Exclusive: Emails of Top NRCC Officials Stolen in Major 2018 Hack." *Politico*, December 4, 2018. https://www.politico.com/story/2018/12/04/exclusive-emails-of-top-nrcc-officials-stolen-in-major-2018-hack-1043309.
[30] Singer, Peter Warren, and Emerson Brooking. "The Online Threat That Cybersecurity Teams Don't Cover." *Quartz at Work*, November 26, 2018. https://qz.com/work/1474702/the-online-threat-that-cybersecurity-teams-dont-cover/.
[31] Perlroth, Nicole. "Security Firm Discovers Cyber-Spy Campaign." *The New York Times*, January 14, 2013. https://bits.blogs.nytimes.com/2013/01/14/security-firm-discovers-global-spy-campaign/.
[32] Jacoby, James. "The Facebook Dilemma (Part One)." PBS FRONTLINE, 2018. https://www.pbs.org/video/the-facebook-dilemma-part-one-s43cuc/.
[33] Jacoby, James. "The Facebook Dilemma (Part Two)." PBS FRONTLINE, 2018. https://www.pbs.org/video/the-facebook-dilemma-part-two-iev1xh/.

Escalating Account Compromises

Online account compromises often occur when cyber criminals manipulate people into sharing their online login credentials (e.g., passwords), a process called *phishing*.[34] Typically, these efforts to steal account login credentials involve *spoofing*—the impersonation of online accounts of organizations that the victim trusts in order to lure the victim into handing over their information to the impostor.[35,36] Phishing is on the rise with more than four in five information security professionals reporting attackers targeted their organization with the technique in 2018, and a 20 percent increase in organizations reporting attacks of *spear phishing*—targeted and personalized phishing—over the previous year.[37] Spear phishing is made easier by the ubiquity of personal information that users share on social media and complemented by the accumulation of stolen personal information, like the 147.9 million personal records stolen in the Equifax breach.[38]

Standard Account Protection Methods

Traditionally, users only protected their online accounts with a password.[39] In an effort to better protect accounts from phishing, many organizations have adopted *multi-factor* (often *two-factor*) *authentication*—proof of identity at login using the combination of more than one thing the user knows, has, or is (see Figure 1).[40,41] The most common two-factor authentication method combines a password (something the user knows) with an ephemeral *one-time pin* or *one-time password* (*OTP*)—numeric access codes that users often receive via text message on their phones (something the user has).[42]

---

[34] Newman, Lily Hay. "Resist Phishing Attacks with Three Golden Rules." *WIRED*, December 9, 2017. https://www.wired.com/story/resist-phishing-attacks/.

[35] Keck, Catie. "Over 80 Percent of Spear Phishing Attacks Involve Brand Impersonation, Security Firm Says." *Gizmodo*, March 21, 2019. https://gizmodo.com/spear-phishing-attacks-are-on-the-rise-security-firm-s-1833455812.

[36] Newman, Lily Hay. "What It's Like When Pro Phishers Assail Your Inbox." *WIRED*, July 4, 2017. https://www.wired.com/story/phishing-attempts-email-inbox/.

[37] Proofpoint. 2019. "State of the Phish." *Wombat Security*. https://info.wombatsecurity.com/hubfs/Wombat_Proofpoint_2019%20State%20of%20the%20Phish%20Report_Final.pdf.

[38] Newman, Lily Hay. "The WIRED Guide to Data Breaches." *WIRED*, December 7, 2018. https://www.wired.com/story/wired-guide-to-data-breaches/.

[39] The conventional advice is to make long, complex, and unique passwords for each account. This is infeasible for many people because of the number of different accounts people own unless they use password management applications, which the County does not currently allow on work computers. Additionally, some advocate frequent password resets like the County requires, but research proves this leads to less secure passwords. Half of users rely on common linkages between updated and old passwords for ease of memory, which researchers demonstrated they could determine 17 percent of the time within five guesses based on an old password. See: Zhang, Yinqian, Fabian Monrose, and Michael K. Reiter. 2010. "The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis." In *17th ACM Conference on Computer and Communications Security*. Chicago, IL: Association for Computing Machinery.

[40] "Back to Basics: Multi-Factor Authentication (MFA)." *National Institute of Standards and Technology*, June 28, 2016. https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.

[41] Many are familiar with multi-factor authentication whenever withdrawing cash from an ATM, which requires a debit card (something someone has) and a PIN (something someone knows).

[42] SatoshiLabs. "Why You Should Never Use Google Authenticator Again: Reasons Why U2F Is Better Than TOTP (One-Time Password)." *Trezor Blog*, October 28, 2016. https://blog.trezor.io/why-you-should-never-use-google-authenticator-again-e166d09d4324.

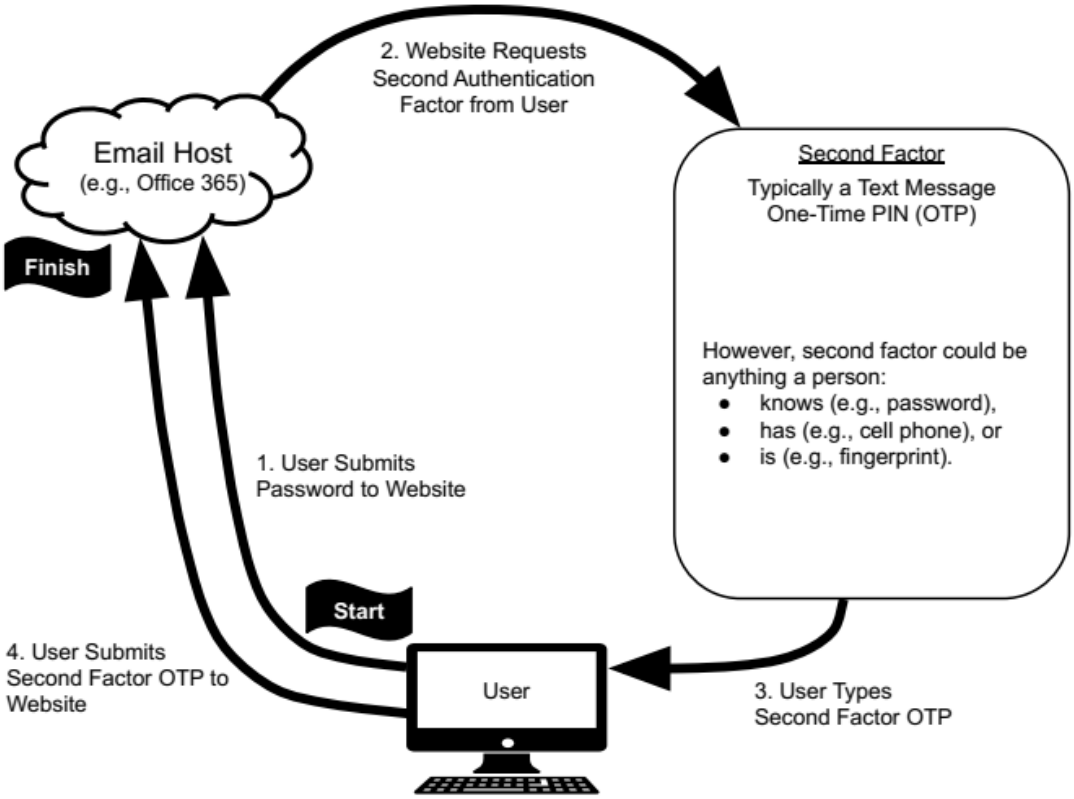

***Figure 1*. Simplified Two-Factor Authentication Process.** Step 1: Users type their passwords on computers and transmit that information to the cloud-based service to which they want to log in (e.g., Office 365). Step 2: That service requests an additional form of identification (e.g., something else users *know* like their mother's maiden name, something users *have* like a previously registered mobile phone, or something users *are* like their fingerprint).[43] Step 3: Users type that second authentication factor on their computers. Step 4: Users verify their identity by submitting the requested information on the website.[44]

[43] Experts agree multi-factor authentication is best when combining two or more forms of identification that are in separate categories of things a user knows, has, or is. See: "Back to Basics: Multi-Factor Authentication (MFA)." *National Institute of Standards and Technology*, June 28, 2016. https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.

[44] Computer and phone icons in Figures 1, 2, and 3 by Patrick Morrison. See: https://thenounproject.com/bluevurt/.

"Man-in-the-Middle" Phishing Can Still Defeat Most Two-Factor Authentication

Security experts agree that even OTP-based multi-factor authentication does not fully protect against phishing.[45,46,47] *Man-in-the-middle* phishing attacks—where people type their passwords on a convincing counterfeit website (e.g., 0ffjce 365 [sic]) and the malicious owner of the counterfeit website simultaneously uses the credentials to log in to a genuine service (e.g., Office 365, see Figure 2)—allow thieves to hijack online accounts with or without OTP-based multi-factor authentication protections.[48,49,50] Freely available malicious software now enables hackers to more easily deploy such attacks, which increases the vulnerability of systems relying on OTP-based multi-factor authentication.[51,52,53] DHS specifically advises against this type of two-factor authentication because of the risk of man-in-the-middle and SIM hijacking attacks (discussed in the following section).[54,55]

[45] Schneier, Bruce. "The Failure of Two-Factor Authentication." *Schneier on Security*, March 15, 2005. https://www.schneier.com/blog/archives/2005/03/the_failure_of.html.
[46] Greenberg, Andy. "So Hey You Should Stop Using Texts for Two-Factor Authentication." *WIRED*, June 26, 2016. https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/.
[47] Grand Jury interview of expert witness who has a Ph.D. in computer science and researches online account security.
[48] Scott-Railton, John, and Katie Kleemola. "London Calling: Two-Factor Authentication Phishing from Iran." *The Citizen Lab*, August 27, 2015. https://citizenlab.ca/2015/08/iran_two_factor_phishing/.
[49] Dunn, John E. "Sneaky Phishing Campaign Beats Two-Factor Authentication." *Naked Security*, December 18, 2018. https://nakedsecurity.sophos.com/2018/12/18/sneaky-phishing-campaign-beats-two-factor-authentication/.
[50] "When Best Practice Isn't Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users." *Amnesty International*, December 19, 2018. https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/.
[51] Cimpanu, Catalin. "New Tool Automates Phishing Attacks That Bypass 2FA." *ZDNet*, January 9, 2019. https://www.zdnet.com/article/new-tool-automates-phishing-attacks-that-bypass-2fa/.
[52] Kan, Michael. "Google: Phishing Attacks That Can Beat Two-Factor Are on the Rise." *PC Magazine*, March 7, 2019. https://www.pcmag.com/news/367026/google-phishing-attacks-that-can-beat-two-factor-are-on-the.
[53] Schlesinger, Jennifer, and Andrea Day. "'You Can't Relax': Here's Why 2-Factor Authentication May Be Hackable." *CNBC*, January 5, 2019. https://www.cnbc.com/2019/01/04/how-secure-is-your-account-two-factor-authentication-may-be-hackable.html.
[54] Department of Homeland Security. "Emergency Directive 19-01 (Migitage DNS Infrastructure Tampering)," January 22, 2019. https://cyber.dhs.gov/ed/19-01/.
[55] Grassi, Paul A., James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, et al. "NIST Special Publication 800-63B (Digital Identity Guidelines)," June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

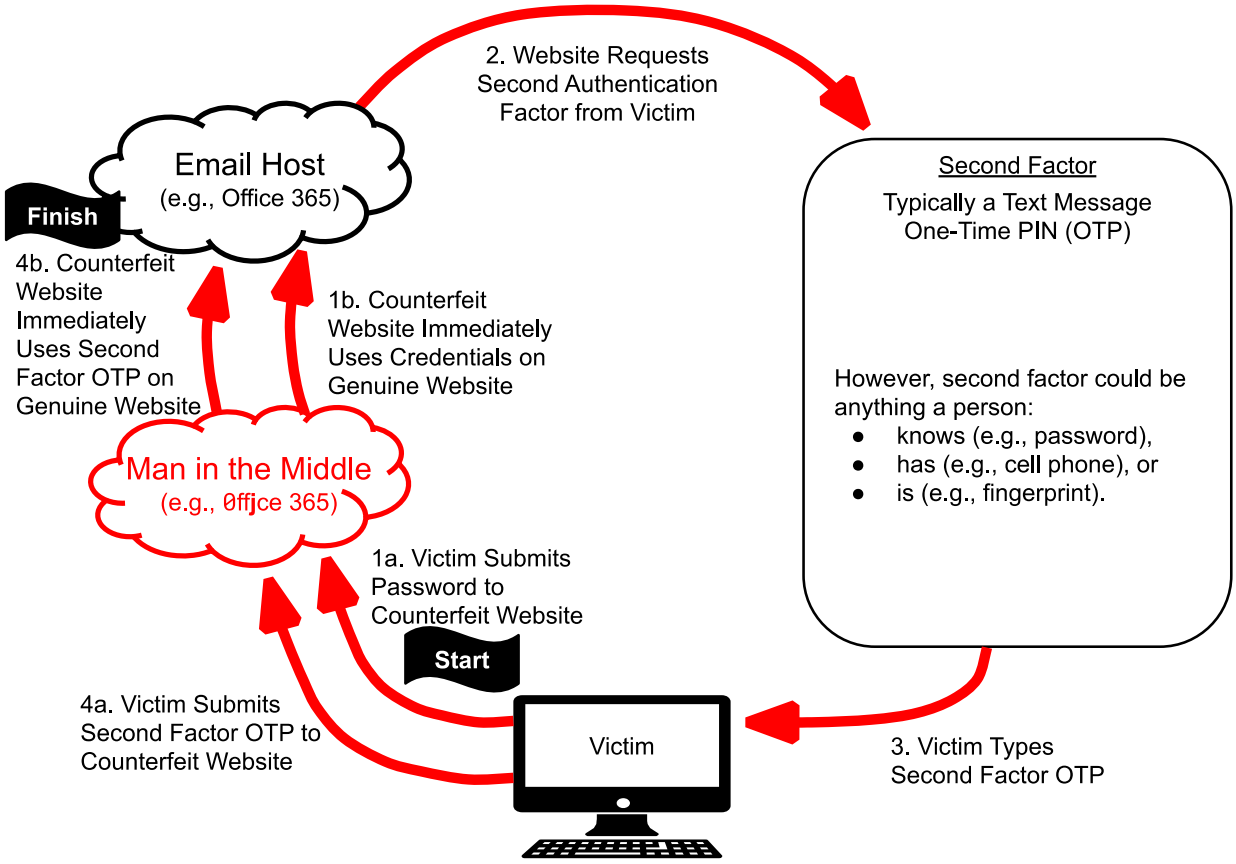

***Figure 2*. Simplified Man-in-the-Middle Phishing Process.** With man-in-the-middle attacks, the only difference with the way two-factor authentication is intended to work (see Figure 1) is that the thieves trick users to enter their passwords on a convincing counterfeit website (e.g., 0ffjce 365 [sic], Step 1a), which simultaneously uses the passwords to gain access to the cloud-based service to which the users intended to log in (Step 1b).

SMS-Based Two-Factor Authentication Has Additional Vulnerabilities

Two-factor authentication using OTPs sent by text messages—illustrated in Figure 3—have additional vulnerabilities.[56,57] There is a rise in reports of *subscriber identity module (SIM) hijacking* or *SIM swapping*—impersonating account holders and deceiving[58] cell phone carrier customer service representatives to redirect a number's service to a different phone in the criminal's control.[59,60,61] By redirecting the phone number, SIM hijackers effectively disable

[56] Krebs, Brian. "Busting SIM Swappers and SIM Swap Myths." *Krebs on Security*, November 7, 2018. https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/.
[57] O'Neill, Patrick Howell. "PSA: SMS 2FA Is Weak AF." Gizmodo, May 10, 2019. https://gizmodo.com/psa-sms-2fa-is-weak-af-1834681656.
[58] Or simply bribing. See: Krebs, Brian. "Busting SIM Swappers and SIM Swap Myths." *Krebs on Security*, November 7, 2018. https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/.
[59] Dreyfuss, Emily. "@deray's Twitter Hack Reminds Us Even Two-Factor Isn't Enough." *WIRED*, June 10, 2016. https://www.wired.com/2016/06/deray-twitter-hack-2-factor-isnt-enough/.

calls and text messages on the victim's phone and then the attackers use the hijacked phone number to reset a victim's password on a website using an "I forgot my password" account recovery option.[62]

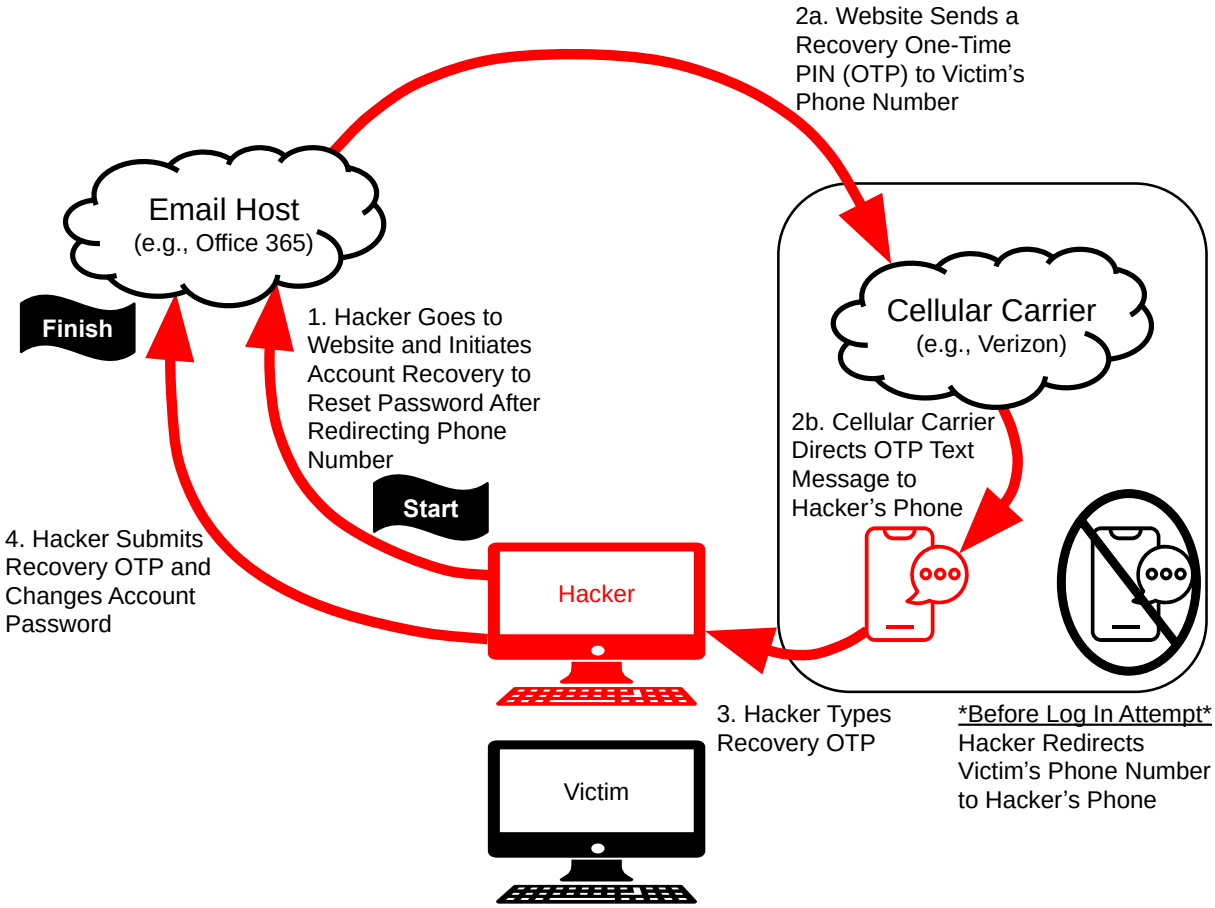

***Figure 3*. Simplified SIM Hijacking Process.** With SMS-based two-factor authentication, criminals can commandeer phone numbers and redirect OTP codes (shown in red) in a method called SIM hijacking.[63]

---

[60] Salonga, Robert. "SIM Swap, Cryptocurrency Busts Highlight New Frontier for Bay Area Tech Cops." *The Mercury News*, September 3, 2018. https://www.mercurynews.com/2018/09/03/sim-swap-cryptocurrency-busts-highlight-new-frontier-for-bay-area-tech-cops/.

[61] Salonga, Robert. "NYC Man Charged in $1 Million Bay Area Cryptocurrency Theft." *The Mercury News*, November 20, 2018. https://www.mercurynews.com/2018/11/20/nyc-man-charged-in-1-million-bay-area-cryptocurrency-theft/.

[62] Popper, Nathaniel. "Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency." *The New York Times*, August 21, 2017. https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html.

[63] In addition to man-in-the-middle and SIM hijacking attacks, criminals can pursue a more resource-intensive attack using a StingRay—a portable device also used by law enforcement that mimics service towers and intercepts voice and text communication in transit. See: Marks, Joseph. "The Cybersecurity 202: Michael Cohen Investigators Relied on Controversial Cell-Tracking Device." *The Washington Post*, March 21, 2019. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/21/the-cybersecurity-202-michael-cohen-investigation-relied-on-controversial-cell-tracking-device/5c92ebe91b326b0f7f38f218/.; and see: Gehman, Julian. "Are the Chinese and Russians Listening to Your Phone Calls?" *The Hill*, December 24, 2018. https://thehill.com/opinion/national-security/422778-are-the-chinese-and-russians-listening-to-your-phone-calls.

DISCUSSION

Public Trust in Election Communication

The DHS (and Not the ACRE) Election Security Website Lists Online Platforms Used for Election Announcements as a High Priority for Protection

When describing the election infrastructure that elections officials need to protect, DHS includes information technology (IT) infrastructure that displays election results.[64] Such infrastructure encompasses all the online communication platforms that the County uses to make election-related announcements—including email, the website, and social media accounts. However, ACRE focuses its attention on the security of voter registration systems and the accuracy of vote tabulation.[65] The ACRE webpage on election security never mentions the security of the online communication platforms used to inform voters leading up to and after elections.[66] One ACRE official assured the Grand Jury that, because there is no sensitive information stored on ACRE's election website, concerns over hacking the website are not high.[67]

DHS Directs Voters to County Websites for Trustworthy Election Information

However, online systems that deliver information about elections are increasingly important. To combat the online spread of disinformation, DHS recommends to voters that they "get election information straight from the source" including your "local election office" and "check [the election office] website" for "accurate information you can trust on the status of your voter registration, polling hours and location, identification requirements, and election results."[68] This advice assumes that these local sources are secure and will deliver accurate information.

The County's Email Security

The County Can Protect Against Email Spoofing with DMARC

Since the 2016 email phishing attack, ISD implemented many security features, including redundant email filtering software that manages the risks of malicious incoming email messages.[69] ISD also protects County email with a popular email security policy, called Sender Policy Framework (SPF).[70] However, DHS issued a binding operational directive (18-01) in 2017 requiring that all federal agencies enhance email security by enabling an additional security policy, called Domain-based Message Authentication, Reporting, and Conformance (*DMARC*).[71] Use of DMARC would complement the County's SPF settings.[72] DHS does not have the

---

[64] Department of Homeland Security. "Election Security." Accessed March 22, 2019. https://www.dhs.gov/topic/election-security.
[65] Grand Jury interviews of multiple ACRE officials.
[66] Assessor-County Clerk-Recorder and Elections. "Election Security and Accuracy." Accessed April 27, 2019. https://www.smcacre.org/post/election-security-and-accuracy.
[67] Grand Jury interview of ACRE official.
[68] Nielsen, Kirstjen, Jeff Sessions, Dan Coats, and Christopher Wray. "Joint Statement on Election Day Preparations," November 5, 2018. https://www.dhs.gov/news/2018/11/05/joint-statement-election-day-preparations.
[69] Grand Jury interview of ISD official.
[70] Grand Jury interview of ISD official.
[71] Department of Homeland Security. "Binding Operational Directive 18-01 (Enhance Email and Web Security)," October 16, 2017. https://cyber.dhs.gov/bod/18-01/.
[72] DMARC is a free email setting that indirectly reduces phishing by eliminating spoofing—a ploy where an attacker falsifies the from header in email to misrepresent belonging to the same organization as the recipient or a trusted

authority to require the County to follow its federal agency directive, and although the current SPF settings and the email filtering software provide many of the DMARC benefits, neither the smcgov.org[73] nor the smcacre.org[74] domains currently protect County email with DMARC.[75] ISD is studying DMARC and intends to use it in the future, but the primary obstacle to its use at this time is the challenge of coordinating system settings with the external partners that also send email on behalf of the County.[76] The federal government recommends DMARC for a broad spectrum of organizations,[77] and DHS strongly encourages its use for elections offices.[78] The City and County of San Francisco already began the process of implementing DMARC email authentication.[79]

One-Time PINs for Multi-Factor Authentication Are Vulnerable to Phishing

Following the successful 2016 phishing attack against a few San Mateo County email accounts, ISD employed a multi-factor authentication service for all County employees.[80] They have several options, but many employees transfer one-time pins (OTPs) sent to them via text message on their previously registered cell phones to verify their identity.[81,82] However, DHS

---

third-party organization, a technique of many cyber criminals when sending phishing emails. The process works by requiring a DMARC-protected organization to verify the authenticity of the source and the integrity of an email before delivering it. Implementing DMARC policies takes time because it requires tracking down the different third-party services used by organizations to send email. See: Kucherawy, Murray S., and Elizabeth Zwicky. "Domain-Based Message Authentication, Reporting, and Conformance (DMARC)." Internet Engineering Task Force, March 18, 2015. https://tools.ietf.org/pdf/rfc7489.pdf; and see: Chandramouli, Ramaswamy, Simson L. Garfinkel, J. Stephen Nightingale, and Scott Rose. "NIST Special Publication 800-177 (Trustworthy Email)," September 2016. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf; and see: DMARC. "Overview." Domain-Based Message Authentication, Reporting and Conformance. Accessed March 22, 2019. https://dmarc.org/overview/; and see: Moorehead, Matt. "How to Explain DMARC in Plain English." Return Path, July 20, 2015. https://blog.returnpath.com/how-to-explain-dmarc-in-plain-english/; and see: Krebs, Brian. "Trump, DNC, RNC Flunk Email Security Test." Krebs on Security, July 25, 2016. https://krebsonsecurity.com/2016/07/trump-dnc-rnc-flunk-email-security-test/comment-page-1/.

[73] dmarcian. "DMARC Inspector (smcgov.org)." Accessed March 22, 2019. https://dmarcian.com/dmarc-inspector/?domain=smcgov.org.

[74] dmarcian. "DMARC Inspector (smcacre.org)." Accessed March 22, 2019. https://dmarcian.com/dmarc-inspector/?domain=smcacre.org.

[75] Grand Jury interview of County official.

[76] Grand Jury interview of ISD official.

[77] Rouge, Phoebe, Sheryl Roth, and Dan Salsburg. "Businesses Can Help Stop Phishing and Protect Their Brands Using Email Authentication," March 2017. https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf.

[78] Cybersecurity and Infrastructure Security Agency. "Domain-Based Message Authentication, Reporting and Conformance." U.S. Department of Homeland Security, March 25, 2019. https://www.dhs.gov/sites/default/files/publications/19_0419_cisa-domain-based-message-authentication-reporting-and-conformance.pdf.

[79] The current settings are "used to collect feedback and gain visibility into email streams without impacting existing flows," meaning DMARC is not actively protecting San Francisco's email yet. See: dmarcian. "DMARC Inspector (sfgov.org)," Accessed on April 25, 2019. https://dmarcian.com/dmarc-inspector/?domain=sfgov.org.

[80] Grand Jury interview of ISD official.

[81] Grand Jury interviews of multiple County officials.

[82] ISD instructs County employees how to secure work email accounts in their annual training. The County forbids the use of personal email for County business and prohibits sending County information to an employee's personal email account. Therefore, the current San Mateo County Information Security Training does not instruct County employees on how to secure personal non-County email accounts. See: Information Services Department. "Information Security Training." San Mateo County; and see: Information Services Department. "Email Policy."

specifically advises against this type of two-factor authentication because of the risk of man-in-the-middle and SIM hijacking attacks.[83,84,85]

The County Can Protect Email Accounts from Phishing with Physical Security Keys

The Grand Jury reviewed expert advice to protect online accounts with *Fast IDentity Online (FIDO) security keys*[86,87,88]—a piece of hardware the size of a house key that owners can carry on their keychain and insert or tap to their computers or phones as part of their online account login process.[89] Among its strengths, FIDO keys scramble the authentication ceremony—the sequence of back-and-forth messages required to confirm a user's identity—so only the legitimate, intended destination can decipher them and so counterfeit phishing websites cannot hijack accounts protected by FIDO keys.[90,91] Unlike traditional OTP-based two-factor authentication, physical FIDO security keys used in two-factor authentication are phishing proof[92] and not susceptible to SIM hijacking.[93,94,95] FIDO keys are not the panacea for security,[96]

San Mateo County, November 7, 2018.
https://cmo.smcgov.org/sites/cmo.smcgov.org/files/ISD%20MEMO%20F2.pdf.

[83] Department of Homeland Security. "Emergency Directive 19-01 (Migitage DNS Infrastructure Tampering)," January 22, 2019. https://cyber.dhs.gov/ed/19-01/.

[84] Grassi, Paul A., James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, et al. "NIST Special Publication 800-63B (Digital Identity Guidelines)," June 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[85] If SMS-based two-factor authentication only occurs while users log in from outside the County network, SIM hijacking is more appealing because bad actors can phish credentials while employees are at work and then only dedicate resources to hijacking phone numbers associated with passwords they successfully phished.

[86] Krebs, Brian. "Google: Security Keys Neutralized Employee Phishing." *Krebs on Security*, July 23, 2018. https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/.

[87] Pegoraro, Rob. "Primer: How to Lock Your Online Accounts with a Security Key." *The Parallax*, December 14, 2018. https://the-parallax.com/2018/12/14/primer-lock-accounts-u2f-security-key/.

[88] Whittaker, Zack. "Cybersecurity 101: Two-Factor Authentication Can Save You from Hackers." *TechCrunch*, December 25, 2018. https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/.

[89] The FIDO keys are currently based on either the universal second factor (U2F) or the newer FIDO2 standards. FIDO2 has the same security benefits of U2F, but can also be configured for passwordless login. See: World Wide Web Consortium, and FIDO Alliance. "W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins," March 4, 2019. https://www.w3.org/2019/03/pressrelease-webauthn-rec.html.

[90] Tong, Jen. "How FIDO U2F Security Keys Work." DevOpsDays Seattle, April 25, 2018. https://www.youtube.com/watch?v=DWrLBwi7ZBA.

[91] FIDO keys have other advantages over phone-based multi-factor authentication, notably they do not require batteries, they do not require an internet connection, they do not require mobile phone ownership, and they do not involve human transcription of authentication codes, which is time consuming and error prone.

[92] There was one case of a Chrome browser feature, WebUSB, creating a vulnerability with one specific class of FIDO key, like the Yubikey Neo model. Google fixed that vulnerability on May 29, 2018 with the release of Chrome 67. See: Johansson, Jesper. "WebUSB in Google Chrome and Responsible Disclosure." *Yubico Blog*, June 13, 2018. https://www.yubico.com/2018/06/webusb-and-responsible-disclosure/.

[93] Grand Jury interview of expert witness who has a Ph.D. in computer science and researches online account security.

[94] Some argue biometrics are equally or even more secure than FIDO keys. However, this assertion discounts the ability of bad actors to spoof an individual's biometrics and the inability to replace that biometric once it is compromised. See: Sanger, David E. "Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says." *The New York Times*, September 23, 2015. https://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html; and see: Winder, Davey. "Samsung Galaxy S10 Fingerprint Scanner Hacked - Here's What You Need To Know." *Forbes*, April 6, 2019. https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/.

which demands constant investment and a culture that encourages reporting vulnerabilities and near misses,[97] but FIDO keys are an important part of an organization's security strategy since over 90 percent of attacks rely on phishing.[98]

Example from Industry: Google Employees Prevent Phishing with FIDO Physical Security Keys

Google researchers found that OTP-based multi-factor authentication, the type many San Mateo County employees use, prevented 96 percent of non-targeted phishing attacks but only prevented 76 percent of spear phishing attacks.[99] Two years ago, Google employees started using FIDO keys instead, and as a result, the company completely eliminated successful phishing attacks against it.[100] Google also reported that, compared with traditional OTP two-factor authentication methods, user experience improved because use of FIDO keys is faster and easier than entering an OTP received via text message on a cell phone, and the company saved "thousands of hours per year in support cost."[101]

The Cost of FIDO Keys for the Elections Staff

The County projects the cost of elections per registered voter will increase from $11.74 last year (FY 2017-18) to $14.50 this year (FY 2018-19),[102] and the Board of Supervisors recently approved an increase of five employees in the next two years to ACRE's current 14-person full-time elections staff.[103] FIDO keys cost approximately $25 each.[104] Therefore, a deployment of 35 FIDO keys, a conservative overestimate of all that would be required to provide one for each of

---

[95] Use of physical FIDO keys should also provide the County with the security justification necessary to extend password lifetimes. See: Evans, Jon. "Password Expiration Is Dead, Long Live Your Passwords." *TechCrunch*, June 2, 2019. https://techcrunch.com/2019/06/02/password-expiration-is-dead-long-live-your-passwords/.

[96] Google recalled its branded FIDO key, named Titan, due to a design flaw in the use of Bluetooth, and Yubico recalled the line of FIDO keys used by the federal government, the YubiKey FIPS Series, due to reduced randomness in its encryption process. Both companies patched their vulnerabilities and quickly replaced the affected keys for free. See: Hoffman, Chris. "Hardware Security Keys Keep Getting Recalled; Are They Safe?" *How-To Geek*, June 14, 2019.

[97] Forbes Technology Council. "10 Cybersecurity Protocols Every Tech Professional Should Follow." *Forbes*, November 28, 2018. https://www.forbes.com/sites/forbestechcouncil/2018/11/28/10-cybersecurity-protocols-every-tech-professional-should-follow/.

[98] DeNisco Rayome, Alison. "Want to Improve Cybersecurity? Try Phishing Your Own Employees." In *Phishing Attacks: Why Is Email Still Such an Easy Target for Hackers?*, edited by Jason Hiner, Steve Ranger, Bill Detwiler, Chris Duckett, Jody Gilbert, Mary Weilage, Conner Forrest, Amy Talbott, and Leah Brown. TechRepublic, 2018. https://www.techrepublic.com/resource-library/whitepapers/phishing-attacks-a-guide-for-it-pros-free-pdf/.

[99] Doerfler, Periwinkle, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, Damon Mccoy, and Kurt Thomas. "Evaluating Login Challenges as a Defense Against Account Takeover." In The World Wide Web Conference (WWW '19), edited by Ling Liu and Ryen White. San Francisco, CA: Association for Computing Machinery, 2019. https://doi.org/10.1145/3308558.3313481.

[100] Krebs, Brian. "Google: Security Keys Neutralized Employee Phishing." *Krebs on Security*, July 23, 2018. https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/.

[101] Lang, Juan, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. "Security Keys: Practical Cryptographic Second Factors for the Modern Web." In *Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2017. doi:10.1007/978-3-662-54970-4_25.

[102] Callagy, Michael P. "FY 2018-19 Adopted Budget." County of San Mateo, September 25, 2018. https://cmo.smcgov.org/sites/cmo.smcgov.org/files/documents/files/FINAL_FY%202018-19%20Adopted%20Budget%20%28with%20hyperlinks%29_0.pdf.

[103] Grand Jury interview of ACRE official.

[104] There are many brands of FIDO keys, but the widely used base-model Yubico Security Key with NFC capability is just $24.50 each. See: "Security Key NFC by Yubico." Yubico. Accessed March 22, 2019. https://www.yubico.com/product/security-key-nfc-by-yubico/#security-key-nfc-2-pack.

the employees that have a role in elections communication,[105] amounts to a one-time cost of about $875, or just 0.2 cents per registered voter.[106]

ACRE's Website Security

ACRE Does Not Protect Its Website with Multi-Factor Authentication: FIDO Keys Can Do That Too

Hackers hijacked and defaced ACRE's election results webpage in 2010.[107] DHS issued an emergency directive (19-01) in 2019 requiring that all federal agency websites mitigate hijacking risks with multi-factor authentication (and discouraging the use of text-message OTPs as a form of multi-factor authentication).[108] While the County is not required to follow the DHS directive, the directive makes clear the importance of using phishing-proof multi-factor authentication to protect ACRE's website. However, ACRE does not protect against unlawful alterations to its smcacre.org website using any form of multi-factor authentication.[109] Free and open-source FIDO libraries exist for a website administrator to enable FIDO authentication for the existing ACRE website.[110]

ACRE Outsources Management of its Website to Vendors Who Must Be at Least as Secure as the County

County departments can manage their websites on their own, they can retain ISD to manage their websites, they can retain a common vendor that several other departments use, or they can choose to retain a different vendor than other departments.[111] Each choice has advantages and disadvantages. ACRE outsources the domain management and hosting of its smcacre.org website to a third-party vendor.[112] Retaining a website vendor increases the possibility that hackers could compromise ACRE's elections website by *island hopping*—a technique used in half of cyber attacks today where a hacker penetrates the weaker security of an organization with whom the ultimate target does business in order to more easily breach the ultimate target.[113,114,115]

---

[105] While departments and the County may wish to consider a wider deployment, this report assumes 35 FIDO keys, which is more than the number of proposed full-time elections staff because the number should include any County employee that communicates on behalf of ACRE (e.g., CMO Chief Communications Officer) or any County employee that has IT administrative privileges over ACRE resources (e.g., senior ISD employees).

[106] The cost estimate of $875 is based on 35 keys and $25 per key. The value of 0.2 cents per registered voter assumes 400,000 registered voters.

[107] Grand Jury interview of County official and supported by corroborating evidence.

[108] Department of Homeland Security. "Emergency Directive 19-01 (Migitage DNS Infrastructure Tampering)," January 22, 2019. https://cyber.dhs.gov/ed/19-01/.

[109] Grand Jury interviews of multiple ACRE officials.

[110] Yubico. "U2F Library in PHP." *GitHub*. Accessed March 22, 2019. https://github.com/Yubico/php-u2flib-server.

[111] Grand Jury interview of County Official.

[112] Grand Jury interviews of multiple ACRE officials.

[113] Halverson, Grace. "Island Hopping: The Latest Security Threat You Should Be Aware Of." *IT Pro*, March 12, 2019. https://www.itpro.co.uk/cyber-attacks/33200/island-hopping-the-latest-security-threat-you-should-be-aware-of.

[114] Carbon Black. "Destructive Cyberattacks Increase Ahead of 2018 Midterm Elections," November 2018. https://www.carbonblack.com/wp-content/uploads/2018/10/carbon-black-quarterly-incident-response-threat-report-november-2018-0119.pdf.

[115] Matteson, Scott. "Carbon Black Incident Response Threat Report: US Elections Are Endangered by Cyberattacks." *TechRepublic*, November 1, 2018. https://www.techrepublic.com/article/carbon-black-incident-response-threat-report-us-elections-are-endangered-by-cyberattacks/.

Social Media Accounts Security

Password Sharing for the County's Social Media Accounts Used for Election Announcements

While the County's ISD sets County email and website policies, ISD does not set policies for the County's use of social media.[116] Therefore, the online security training materials produced by ISD do not make any recommendations to protect against hacking of official County social media accounts.[117] The County Manager's Office (CMO) manages the official San Mateo County social media accounts.[118] CMO also offers assistance to County departments as they establish their own official social media accounts and advice on the management and utilization of existing official departmental social media accounts.[119] Some departments choose not to manage social media accounts on particular platforms, and so they send CMO messages for publication on the corresponding official San Mateo County social media webpages.[120] For example, ACRE does not manage its own Facebook or Nextdoor accounts, and instead, it sends some messages to CMO and asks them to publish the notices on the San Mateo County Facebook and Nextdoor webpages.[121] The San Mateo County Departmental Social Media Policy produced by CMO requires that multiple employees (limited to department heads, their designees, and any department social media managers) share official social media account passwords in case the primary social media manager is unavailable.[122,123] ACRE officials gave the same reason for sharing account passwords.[124] Table 1 lists the social media accounts controlled by ACRE and CMO that the County uses to broadcast election announcements.

Table 1. Social Media Accounts Used to Broadcast Election Announcements.[125]

Platform	Page	SMC Dept.	Shared Passwords	Two-Factor Protection
Facebook	facebook.com/CountyofSanMateo	CMO	Yes	SMS OTP
Instagram	instagram.com/smcvote	ACRE	Yes	None
Nextdoor	nextdoor.com/agency-detail/ca/san-mateo-county/county-of-san-mateo	CMO	Yes	None[126]
Twitter	twitter.com/smcvote	ACRE	Yes	None
YouTube	youtube.com/user/democracylive	ACRE	Yes	None

[116] Grand Jury interview of County official.
[117] Information Services Department. "Information Security Training." San Mateo County.
[118] Grand Jury interviews of multiple County officials.
[119] Grand Jury interviews of multiple County officials.
[120] Grand Jury interviews of multiple County officials.
[121] Grand Jury interviews of multiple County officials.
[122] County Manager's Office. "San Mateo County Departmental Social Media Policy." San Mateo County. April 2015.
[123] Grand Jury interviews of multiple County officials.
[124] Grand Jury interviews of multiple County officials.
[125] ACRE formerly hosted pictures with a Flickr account (flickr.com/photos/28783904@N05), but since the account remains unchanged since July 2008 ACRE should consider archiving those pictures elsewhere and deleting the account.
[126] Multi-factor authentication is currently unavailable on Nextdoor.

Sharing passwords was a common practice years ago, but is not necessary on Facebook,[127] Twitter,[128] Instagram,[129] and YouTube,[130] because all of these platforms now allow *multi-user administration*—a configuration where two or more employees can each control an official County social media page with their individual accounts. Password sharing for social media accounts in an organization often inhibits the organization from enabling multi-factor authentication.[131] Organizations that share passwords also run a higher risk of disgruntled workers giving the shared password to unauthorized individuals due to the lack of accountability or former employees still having the ability to control a shared account after their employment ends if the password is not changed.[132]

Multi-Factor Authentication for the County's Social Media Accounts Used for Election Announcements

The San Mateo County Departmental Social Media Policy produced by CMO also does not make any recommendations about using multi-factor authentication.[133] Facebook, Twitter, and YouTube support the same FIDO-key multi-factor authentication described previously.[134,135] Hackers demonstrated the ability to hijack social media accounts without FIDO-key authentication to spread disinformation,[136] even to make political statements on behalf of trusted organizations.[137,138]

Cyber Hygiene Practices

Opportunity to Broaden Election Security Perspective

Many elections employees have some security responsibilities.[139] However, ACRE intentionally silos many security issues on a need-to-know basis in an effort to contain risk.[140] For instance,

---

[127] "Add People to Your Ad Account." *Facebook*. Accessed March 22, 2019. https://www.facebook.com/business/help/195296697183682.
[128] "Multi-User Login." *Twitter*. Accessed March 22, 2019. https://business.twitter.com/en/help/troubleshooting/multi-user-login-faq.html.
[129] "Manage Roles on a Shared Instagram Account." *Facebook*. Accessed March 22, 2019. https://www.facebook.com/help/218638451837962.
[130] "Invite A User to Manage Content." *YouTube*. Accessed March 22, 2019. https://support.google.com/youtube/answer/4524878.
[131] Singh Masuta, Kamal. "Three Simple Steps to Protect Shared Twitter Accounts from Hackers." Committee to Protect Journalists, March 28, 2016. https://cpj.org/blog/2016/03/three-simple-steps-to-protect-shared-twitter-accou.php.
[132] DeNisco Rayome, Alison. "Why Businesses Fear Cyberattacks from Ex-Employees More Than Nation States." *TechRepublic*, February 27, 2019. https://www.techrepublic.com/article/why-businesses-fear-cyberattacks-from-ex-employees-more-than-nation-states/.
[133] County Manager's Office. "San Mateo County Departmental Social Media Policy." San Mateo County. April 2015.
[134] Nitrokey. "Social." *USB-Dongle Authentication*. Accessed May 31, 2019. https://www.dongleauth.info/#social.
[135] Nitrokey. "Entertainment." USB-Dongle Authentication. Accessed May 31, 2019. https://www.dongleauth.info/#entertainment.
[136] Dreyfuss, Emily. "@deray's Twitter Hack Reminds Us Even Two-Factor Isn't Enough." *WIRED*, June 10, 2016. https://www.wired.com/2016/06/deray-twitter-hack-2-factor-isnt-enough/.
[137] Ciaccia, Chris. "McDonald's Twitter Account Hacked, Blasts Trump." *Fox News*, March 16, 2017. https://www.foxnews.com/tech/mcdonalds-twitter-account-hacked-blasts-trump.
[138] Singer, Peter Warren, and Emerson Brooking. "The Online Threat That Cybersecurity Teams Don't Cover." *Quartz at Work*, November 26, 2018. https://qz.com/work/1474702/the-online-threat-that-cybersecurity-teams-dont-cover/.
[139] Grand Jury interview of multiple ACRE officials.

ACRE's elections supervisor in charge of security is not involved in most of the security decisions ACRE's Information Technology group makes.[141]

Availability of Free DHS Cybersecurity Services

DHS offers free cybersecurity advisories to state and local governments through a program called the Multi-State Information Sharing and Analysis Center, which one of the ISD employees interviewed and one of the ACRE employees interviewed acknowledged they receive.[142,143] However, no ACRE employee acknowledged utilizing any of the free DHS consulting tailored to each elections office in the catalog of services for election infrastructure, listed in Table 2. In interviews, one ACRE employee said ISD is responsible for procuring other DHS services[144] and another ACRE employee explained how ACRE would work closely with ISD if DHS identified network vulnerabilities,[145] while an ISD employee explained how it encourages and would collaborate with ACRE to improve ACRE's security, but subscribing to DHS services for the sole benefit of one department—ACRE—is up to ACRE to initiate.[146,147] The same ISD employee recalled learning that a nearby county utilizes DHS's election-specific services.[148] For its part, DHS makes it clear that they can only provide cybersecurity assistance "to election officials who request it."[149]

---

[140] Grand Jury interview of ACRE official.
[141] Grand Jury interview of ACRE official.
[142] Grand Jury interviews of multiple County officials.
[143] DHS also refers to the program as EI-ISAC, see: Election Infrastructure Subsector Government Coordinating Council. "DHS Election Infrastructure Security Funding Consideration." U.S. Department of Homeland Security, June 13, 2018. https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final_0.pdf.
[144] Grand Jury interview of ACRE official.
[145] Grand Jury interview of ACRE official.
[146] A department must still "work with ISD to validate, implement, and/or manage" any new technology service that impacts the County's network.
[147] Grand Jury interview of ISD official.
[148] Grand Jury interview of ISD official.
[149] National Protection and Programs Directorate. "DHS Election Infrastructure Security Resource Guide." U.S. Department of Homeland Security, July 10, 2018. https://www.dhs.gov/sites/default/files/publications/Election%20Resource%20Guide%20July%202018_508.pdf.

Table 2. DHS Cybersecurity Services Offered to Elections Divisions.[150]

Program	**Quoted Description of No-Cost, Voluntary Service**
Cyber Resilience Review	interview-based assessment to evaluate... operational resilience and cybersecurity practices… to manage cyber risk during normal operations and times of operational stress and crisis
External Dependencies Management Assessment	interview-based assessment to evaluate… management of… risks arising from external dependencies within the information and communication technology (ICT) supply chain
Cyber Infrastructure Survey	evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience
Phishing Campaign Assessment	evaluates… susceptibility and reaction to phishing emails. [the service is] meant to provide guidance, measure effectiveness, and justify resources needed to defend against spear-phishing
Risk and Vulnerability Assessment	designed to determine whether and by what methods an adversary can defeat network security controls
Vulnerability Scanning *(formerly known as Cyber Hygiene scanning)*	incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which… increas[es] the Nation's overall resiliency
Validated Architecture Design Review	encompasses architecture and design review, system configuration, log file review, and sophisticated analysis of network traffic to… identify anomalous (and potentially suspicious) communication flows
Cybersecurity Evaluation Tool	evaluate[s]… cybersecurity posture against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner

Opportunity for Internal Vulnerability Assessments

ISD does conduct network vulnerability assessments for the entire County under a "Vulnerability Scanning" program DHS offers to state and local governments like the one listed in Table 2 for elections divisions.[151] These assessments are automated scans of devices on the network, not an investigation into behavioral sources of network vulnerability.[152] "[M]any of the most harmful attacks on computer systems originate with an attacker targeting a human being."[153] The County

[150] Department of Homeland Security. "DHS Cybersecurity Services Catalog for Election Infrastructure." U.S. Election Assistance Commission. Accessed March 23, 2019. https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf.
[151] Grand Jury interview of ISD official.
[152] Grand Jury interview of ISD official and supported by corroborating evidence.
[153] Lin, Herbert, Alex Stamos, Nate Persily, and Andrew Grotto. "Increasing the Security of the U.S. Election Infrastructure." In *Securing American Elections: Prescriptions for Enhancing the Integrity and Independence of the 2020 U.S. Presidential Elections and Beyond*, edited by Michael McFaul, 17–26. Stanford University Cyber Policy Center at the Freeman Spogli Institute for International Studies, 2019. https://bit.ly/StanfordCyberPolicy.

Controller's Office "also performs internal audits of departments' operations."[154,155] One of the auditors in the Internal Audit Division of the Controller's Office specializes in information technology.[156] The Internal Audit Division conducts limited-scope cyber hygiene assessments during some internal audits, but it has not conducted such an audit of the ACRE Elections Division.[157] Due to resource and expertise constraints, the Controller's Office generally limits the scope of cyber hygiene assessments to things like software update practices.[158] However, both the Controller's Office and ISD worked together in the past to conduct cyber hygiene assessments that evaluated security practices and compliance with information technology policies.[159] Officials from both the Controller's Office and ISD indicated they would be amenable to working together to review the security practices and compliance of ACRE.[160]

[154] Controller's Office. "Controller's Office." County of San Mateo. Accessed June 4, 2019. https://controller.smcgov.org/.
[155] Grand Jury interview of Controller's Office official.
[156] Grand Jury interview of Controller's Office official.
[157] Grand Jury interview of Controller's Office official.
[158] Grand Jury interview of Controller's Office official.
[159] Grand Jury interview of multiple County officials.
[160] Grand Jury interviews of Controller's Office and ISD officials.

FINDINGS

Vulnerability of Public Trust in Election Communications

F1. The veracity of the County's election broadcasts on any ACRE or CMO online communication platform is important to the public's trust in the electoral process.

F2. Unlike DHS,[161] ACRE does not include the security of online election communications when describing election security on its website.[162]

F3. Protecting online communication platforms with multi-factor authentication that is susceptible to SIM hijacking, phishing, and man-in-the-middle attacks—as is the case with the use of one-time PINs (OTPs) sent to cell phones—exposes the County to election disinformation attacks.

Vulnerability of the County's Email

F4. Although the County implemented several email security protections that provide many of the DMARC benefits following a 2016 phishing attack, the County's email security practices do not follow DHS guidelines for federal agencies due to the absence of complementing DMARC protection.

F5. The County utilizes multi-factor authentication methods for its email that remain susceptible to SIM hijacking, phishing, and man-in-the-middle attacks.

Vulnerability of ACRE's Website

F6. ACRE's website security practices do not follow DHS guidelines for federal agencies requiring the use of multi-factor authentication protection by users who have the system permissions to alter the ACRE webpages.

F7. ACRE outsources the domain management and hosting of its smcacre.org website to a third-party vendor.

Vulnerability of Social Media Accounts

F8. The San Mateo County Information Security Training produced by ISD does not make any recommendations for security practices of official County social media accounts.

F9. The San Mateo County Departmental Social Media Policy produced by CMO requires that multiple employees share official social media account passwords.

---

[161] Department of Homeland Security. "Election Security." Accessed March 22, 2019. https://www.dhs.gov/topic/election-security.
[162] Assessor-County Clerk-Recorder and Elections. "Election Security and Accuracy." Accessed April 27, 2019. https://www.smcacre.org/post/election-security-and-accuracy.

F10. ACRE and CMO employees share passwords to their official social media accounts listed in Table 1 with multiple employees within their offices.

F11. The San Mateo County Departmental Social Media Policy produced by CMO does not make any recommendations about using multi-factor authentication to protect against an unlawful takeover of social media accounts.

F12. The ACRE and CMO social media accounts listed in Table 1, with the exception of the CMO Facebook page, do not use multi-factor authentication.

Status of Cyber Hygiene

F13. ACRE and ISD could strengthen their coordination of the evaluation and addition of security features to address election security.

F14. ISD utilizes a DHS "Vulnerability Scanning" service for the entire County, but ACRE does not utilize any of the other seven free elections-specific DHS services listed in Table 2.

F15. ISD runs network vulnerability assessments ("Vulnerability Scanning") for the County devices, but does not audit the practices of employees to identify behavioral sources of network vulnerability.

F16. The Internal Audit Division of the County Controller's Office "performs internal audits of departments' operations," which has sometimes included cyber hygiene assessments.

F17. The Internal Audit Division of the County Controller's Office has not performed a cyber hygiene assessment of the Elections Division of ACRE.

RECOMMENDATIONS

Protect the Public Trust in Election Communication

R1. **Incorporate Communications into Election Security Definition:** ACRE should adopt a policy that defines election security to include the security of the ACRE website, ACRE staff email accounts, social media accounts used for ACRE announcements, and other platforms ACRE uses for publishing election announcements. ACRE should implement this recommendation by December 31, 2019.

R2. **Publish Updated Security Policy:** ACRE should update the ACRE website's written descriptions of the election security[163] to incorporate the policy resulting from R1 on the security of election communications in addition to the current focus on security of (a) registration, (b) vote casting, and (c) results tabulation. ACRE should implement this recommendation by June 30, 2020.

Protect the County's Email

R3. **Prevent Spoofing with DMARC:** ISD, CMO, and ACRE should improve email security for employees involved in election announcements by configuring and enabling DMARC for at least the smcacre.org and smcgov.org domains. ISD, CMO, and ACRE should implement this recommendation by June 30, 2020.

R4. **Combat ACRE Email Account Phishing with FIDO Keys:** ACRE should provide FIDO physical security keys to each of its permanent elections employees and require the use of those FIDO keys as part of their multi-factor authentication for accessing their County email accounts. ACRE should implement this recommendation by December 31, 2019.

R5. **Combat Other Email Account Phishing with FIDO Keys:** ACRE should identify County employees outside of ACRE that have a role in election announcements (e.g., Chief Communications Officer, senior ISD employees, etc.) and ask that the departments of the identified employees provide FIDO physical security keys to each of the identified employees and require the use of those FIDO keys as part of their multi-factor authentication for accessing their County email accounts. ACRE should complete this recommendation by December 31, 2019.

Protect ACRE's Website

R6. **Combat Website Account Phishing with FIDO Keys:** ACRE should require all County employees whose user accounts allow them to alter the ACRE website[164] to use FIDO physical security keys as part of their multi-factor authentication. ACRE should implement this recommendation by December 31, 2019.

---

[163] Assessor-County Clerk-Recorder and Elections. "Election Security and Accuracy." Accessed April 27, 2019. https://www.smcacre.org/post/election-security-and-accuracy.

[164] Including all accounts capable of directly editing the ACRE website, managing the smcacre.org domain, and any administrator account capable of managing other accounts that can edit the website or manage the domain.

R7. **Combat Island Hopping with FIDO Key Vendor Requirement:** ACRE and ISD should require employees and contractors of any vendor that hosts the ACRE website to use FIDO physical security keys as part of their multi-factor authentication.[165] ACRE and ISD should implement this recommendation by December 31, 2019.

Protect the Social Media Accounts

R8. **Stop Sharing Social Media Account Passwords:** ACRE and CMO should implement procedures whereby communications staff manage official County social media accounts with multi-user administration, and no employees share social media account passwords. ACRE and CMO should implement this recommendation by October 31, 2019.

R9. **Request FIDO Key Feature If Not Available:** ACRE and CMO should jointly draft and send a FIDO-key feature request citing this report to the social media companies used by the County to broadcast election announcements, but that do not currently offer FIDO account security protections—especially Instagram and Nextdoor. ACRE and CMO should implement this recommendation by August 31, 2019.

R10. **Combat ACRE Social Media Account Phishing with FIDO Keys:** ACRE should require any employee social media accounts capable of administering the official ACRE social media pages listed in Table 1 to use FIDO physical security keys as part of their multi-factor authentication. ACRE should implement this recommendation by December 31, 2019.

R11. **Combat SMC Social Media Account Phishing with FIDO Keys:** CMO should require any employee social media accounts capable of administering the official San Mateo County social media pages listed in Table 1 to use FIDO physical security keys as part of their multi-factor authentication. CMO should implement this recommendation by December 31, 2019.

Improve Cyber Hygiene

R12. **Coordinate Election Security with Interdepartmental Working Group:** ACRE and ISD should create an election security working group that meets periodically and is responsible for evaluating and improving the security of elections (a) registration, (b) vote casting, (c) results tabulation, and (d) communication within San Mateo County. ACRE and ISD should implement this recommendation by December 31, 2019.

R13. **Evaluate Free DHS Elections Security Assistance Programs:** ACRE and ISD election-security working group should evaluate the benefits of having all members of the election-security working group participate in any of the free DHS elections security assistance

[165] At a minimum for any user account with a public portal capable of administering the ACRE website, any virtual private network (VPN) account that can access a private portal capable of administering the ACRE website, any account capable of managing the smcacre.org domain, and every email account within the vendor organization.

programs listed in Table 2. ACRE and ISD should implement this recommendation by February 3, 2020.

R14. **Offer Behavioral Cyber Hygiene Audits:** ISD and the County Controller's Office should develop a behavioral auditing program consisting of sampling the day-to-day routines and security practices of employees, contractors, and/or vendors and offer to audit each department within the County periodically to (1) evaluate compliance with existing cyber hygiene policies and (2) provide proactive advice on cyber hygiene improvements that could inform new policies. ISD and the Controller's Office should begin to implement this recommendation by offering to audit ACRE and ISD (itself) in time to finish by February 3, 2020.

REQUEST FOR RESPONSES

Pursuant to Penal Code Section 933.05, the Grand Jury requests responses to the previously stated findings and recommendations from:

- The County of San Mateo Board of Supervisors, on behalf of:
  - The County Manager's Office (CMO)
  - The Information Services Department (ISD)
- The San Mateo County Assessor-County Clerk-Recorder and Elections Office (ACRE)
- The San Mateo County Controller's Office

The governing body indicated above should be aware that the comment or response of the governing body must be conducted subject to the notice, agenda, and open meeting requirements of the Brown Act.

METHODOLOGY

The Grand Jury:

- reviewed all documents, websites, and articles with full citations in the footnotes of the body of this report and the key references listed in an abridged bibliography at the end of this report,
- visited and toured the elections headquarters at 40 Tower Road, and
- interviewed 13 San Mateo County officials and one expert from industry further described below.

County Documents

- Callagy, Michael P. "FY 2018-19 Adopted Budget." County of San Mateo, September 25, 2018. https://cmo.smcgov.org/sites/cmo.smcgov.org/files/documents/files/FINAL_FY%202018-19%20Adopted%20Budget%20%28with%20hyperlinks%29_0.pdf.
- Church, Mark. "San Mateo County Election Infrastructure Security." *Memo to Board of Supervisors*, March 20, 2018.
- County Manager's Office. "San Mateo County Departmental Social Media Policy." San Mateo County, April 2015.

- Information Services Department. “Email Policy.” San Mateo County, November 7, 2018. https://cmo.smcgov.org/sites/cmo.smcgov.org/files/ISD%20MEMO%20F2.pdf.
- Information Services Department. “Information Security Training.” San Mateo County.

Site Tours

- The San Mateo County elections headquarters at 40 Tower Road

Interviews

- Officials within the office of Assessor-County Clerk-Recorder and Elections (ACRE)
- Official within the Controller’s Office
- Officials within the County Manager’s Office (CMO)
- Officials within the Information Services Department (ISD)
- Expert witness who has a Ph.D. in computer science and contributes to account security efforts within one of the largest global technology companies headquartered nearby

ABRIDGED BIBLIOGRAPHY

Camp, Joseph. "How Secure Are the Midterm Elections?" United States: PBS NewsHour, 2018. https://www.youtube.com/watch?v=r6UQuz5tVV0.

Ciaccia, Chris. "McDonald's Twitter Account Hacked, Blasts Trump." *Fox News*, March 16, 2017. https://www.foxnews.com/tech/mcdonalds-twitter-account-hacked-blasts-trump.

Department of Homeland Security. "DHS Cybersecurity Services Catalog for Election Infrastructure." *U.S. Election Assistance Commission*. Accessed March 23, 2019. https://www.eac.gov/assets/1/6/DHS_Cybersecurity_Services_Catalog_for_Election_Infrastructure.pdf.

Department of Homeland Security. "Election Security." Accessed March 22, 2019. https://www.dhs.gov/topic/election-security.

Doerfler, Periwinkle, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, Damon Mccoy, and Kurt Thomas. "Evaluating Login Challenges as a Defense Against Account Takeover." In *The World Wide Web Conference (WWW '19)*, edited by Ling Liu and Ryen White. San Francisco, CA: Association for Computing Machinery, 2019. https://doi.org/10.1145/3308558.3313481.

Greenberg, Andy. "So Hey You Should Stop Using Texts for Two-Factor Authentication." *WIRED*, June 26, 2016. https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/.

Johnson, Jeh. "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector." *Department of Homeland Security*, January 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

Krebs, Brian. "Busting SIM Swappers and SIM Swap Myths." *Krebs on Security*, November 7, 2018. https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths/.

Krebs, Brian. "Google: Security Keys Neutralized Employee Phishing." *Krebs on Security*, July 23, 2018. https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/.

Lang, Juan, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. "Security Keys: Practical Cryptographic Second Factors for the Modern Web." In *Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2017. doi:10.1007/978-3-662-54970-4_25.

Newman, Lily Hay. "The WIRED Guide to Data Breaches." *WIRED*, December 7, 2018. https://www.wired.com/story/wired-guide-to-data-breaches/.

Nielsen, Kirstjen, Jeff Sessions, Dan Coats, and Christopher Wray. "Joint Statement on Election Day Preparations," November 5, 2018. https://www.dhs.gov/news/2018/11/05/joint-statement-election-day-preparations.

Parks, Miles. "Florida Governor Says Russian Hackers Breached 2 Counties In 2016." *NPR*, May 14, 2019. https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016.

Schneier, Bruce. "The Failure of Two-Factor Authentication." *Schneier on Security*, March 15, 2005. https://www.schneier.com/blog/archives/2005/03/the_failure_of.html.

Whittaker, Zack. "Cybersecurity 101: Two-Factor Authentication Can Save You from Hackers." *TechCrunch*, December 25, 2018. https://techcrunch.com/2018/12/25/cybersecurity-101-guide-two-factor/.

Wofford, Benjamin. “The Hacking Threat to the Midterms Is Huge. And Technology Won’t Protect Us.” *Vox*, October 25, 2018. https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting.

“Nielsen Says US Ready for Cybersecurity Trouble.” United States: Associated Press, 2018. https://www.youtube.com/watch?v=UneZJ1rNxH4.

“When Best Practice Isn’t Good Enough: Large Campaigns of Phishing Attacks in Middle East and North Africa Target Privacy-Conscious Users.” *Amnesty International*, December 19, 2018. https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/.

Issued: July 24, 2019