

Your Cybersecurity Handbook: Tips and Tricks to Stay Safe

Contents

- 3 Introduction
- 4 You and Cyber + Introductory Quiz
- 5 **Your Cyber Briefing: Need to Know**
- 7 Shrink Your Security Blind Spots
- 9 Crossword Puzzle
- 11 How to Beat the Bad Password Blues
- 12 Passwords and Protections 101
- 15 Telework Demands Secure Connections
- 17 **Virtual Meeting Tips and Tricks**
- 19 The 3 Essentials of Remote Cybersecurity
- 20 Physical Security in the Digital Era
- 23 Challenges for Security Personnel Have Grown: What They Need
- 27 Building Your Security for the Modern Era
- 28 Phishing, Ransomware and Common Threats
- 31 Dealing With Complexity in a Tangled World
- 35 How We Can Get Through Today's Cyberthreats Together
- 36 **Cybersecurity Spotlight: Login.Gov**
- 39 The Foundation for Future-Facing Cybersecurity
- 40 Logging Off: Tips for Securing Your Work and Your Family
- 42 A Clarion Call: Kill the Password
- 43 Conclusion + Acknowledgments

Introduction

PWK. *Phone. Wallet. Keys.* That simple mnemonic has changed my life, maybe not with the grandiose spices of fortune and fame, but certainly by eliminating the angst of panicky moments, heartache and forgotten possessions.

I'll admit, I'm not the most organized person. So when I visited my lifelong friend in New York and she perceptively noticed a few frantic pocket taps and brushes symptomatic of vacation anxiety, she asked me, "PWK?" I had no idea what that meant.

She explained to me that she always made sure she had everything before leaving the apartment by reciting "PWK" in her head. Phone. Wallet. Keys.

That was a few years ago, and I haven't lost my phone, wallet or keys since.

So, you ask, *what does this have to do with cybersecurity?*

Let's face it. We, as human beings, are programmed to be forgetful. And needing a gajillion passwords to access all of our apps, devices, services, accounts and information leeches what little battery power we have left from life's trials of the day.

We could be forgiven for a dose of annoyance at all the burdensome cybersecurity steps. There has to be an easier way. If only there was a PWK for cyber.

This guide is going to give you a touch of that. We've sourced government documents from federal, state and local agencies that teach cybersecurity softly, instead of hitting you over the head with a 20-page stack of legalistic regulations and requirements. In the process, you'll learn definitions, best practices and crucial answers in an interactive manner. You might even have fun doing so. I know I did while planning, researching and writing this resource.

Before I let you through the gates of this guide, there's another note I'd be remiss to omit. Many of us are working from home right now. Even if you're not, you're still taking extra precautions. Threats are on the rise, digital and otherwise. This is life in a pandemic. The guide will cover that.

Finally, thank you to Maricopa County, Arizona; the Federal Trade Commission (FTC); the Cybersecurity and Infrastructure Security Agency (CISA); and North Dakota. Through online web pages or internal best practices and memos shared with GovLoop, these cybersecurity stewards and trailblazers carried the bulk of this guide. Their advice was so valuable and well-written, I didn't even have to decode any cyber jargon most of the time.

With that being said, enjoy. Go explore cybersecurity, and I hope you'll find your own *PWK* on the way.



Isaac Constans
Senior Staff Writer
GovLoop

Input a password with 10-15 characters, one special key and at least one capital and one lowercase letter. Your password must be changed every six months.

.....

Select all images containing traffic lights.



Never access personal information on a public network.

You and Cyber

We know that at work, your agency or organization is hammering the importance of cybersecurity down your throat. It can be a brutal, boring and belaboring exercise when done wrong. And even when done right, let's be real, it's still more red tape.

In a recent GovLoop survey, 23% of local government respondents said cybersecurity is a top three priority for their agencies. Federal employees told the same story, to the tune of 23%. But only 3% and 7%, respectively, of local and federal government employees said cybersecurity is a top three item they're interested in learning about.

So what we have is a misalignment. Agencies care (rightfully) about cybersecurity. But employees? It's not at the top of their lists.

The facts are plain. Agencies need a way to destigmatize cybersecurity and engage employees if they want the million-dollar ransoms to stop; employee negligence is the biggest threat to cybersecurity, after all.

It's not that employees shouldn't care, either. Cybersecurity is a part of job performance! And the principles of caution at work apply to home as well, especially in this digital age. We all know someone who's had their identity, bank information or digital accounts stolen. It's no fun getting that back.

The solution, then, naturally follows. People need to care more about cybersecurity – one way or another. Take this beyond the annual test and to the grounds of regular, day-to-day work. If that means activities, games and prizes, then so be it.

Simply: Make cybersecurity fun.

Disclaimer: Some of the information in this guide has been sourced directly from government documents with the permission of the publishing body or as a public document. Those instances are noted. Minor changes have been made for readability, style and additional information.

Introductory Quiz

Let's go over some cybersecurity basics. Take this quiz from the FTC to gauge where you're at. Answers are on the following page.

1. Which of the following should you do to restrict access to your files and devices?

- A. Update your software once a year
- B. Share passwords only with colleagues you trust
- C. Have your staff members access information via an open Wi-Fi network
- D. Use multifactor authentication

2. True or false: Backing up important files offline, on an external hard drive or in the cloud, will help protect your business in the event of a cyberattack.

3. Which people in an organization should be responsible for cybersecurity?

- A. Leadership. They run the place, so they need to know cybersecurity basics and put them in practice to reduce the risk of cyberattacks.
- B. IT specialists. They are in the best position to know and promote cybersecurity.
- C. Managers. They are responsible for making sure staff members are following the right practices.
- D. All staff members. Everyone should know some cybersecurity basics to reduce the risk of cyberattacks.

4. True or false: Cybercriminals only target large organizations.

5. What is the best way to secure your personal router?

- A. Change the default name and password of the router
- B. Turn off the router's remote management
- C. Log out as the administrator once the router is set up
- D. All of the above

Answer Key

1. **D.** Requiring multifactor authentication to access areas of your network that include sensitive information helps safeguard important data. This requires additional steps beyond logging in with a password – like a temporary code on a smartphone, or a key that’s inserted into a computer.
2. **True.** Backing up important files offline can help protect them in case of a cyberattack.
3. **D.** All staff should know to follow basic cybersecurity practices – and everyone should get regular training. This is done by cultivating a culture of cybersecurity.
4. **False.** Cybercriminals target organizations of all sizes.
5. **D.** To help secure your router, change the default name and password, turn off remote management and log out as the administrator when not performing administrative functions.

Your Cyber Briefing: Need to Know

Cybersecurity Glossary: Common Terms

These are the cybersecurity terms and concepts that Maricopa County deemed necessary for its employees to know and understand. See what you recognize.

Security Superheroes

Encryption: The process of encoding data to prevent theft. Users can only access the data with a digital key.

Why it matters: Encryption makes it harder for bad guys to read your data.

Firewall: A defensive technology designed to keep out intruders. Firewalls can be hardware- or software-based.

Why it matters: This defensive layer essentially “circles the wagons” around your network.

Multifactor Authentication: Requiring users to provide at least two ways of identifying themselves, such as with a code provided in an email, text or voicemail in addition to a password or passcode.

Why it matters: Many attackers using your information are unable to get past a second round of authentication, even if they have the tools to unlock the first set of barriers.

Virtual Private Network (VPN): A tool that allows users to remain anonymous while using the internet by masking the location and encrypting traffic.

Why it matters: Being anonymous is a great way to keep out of hackers’ hands.

Cloud: A technology that allows us to access files and services through the internet from anywhere in the world. Technically speaking, it’s a collection of computer servers with large storage capabilities that remotely serve requests.

Why it matters: Cybersecurity professionals have the daunting task of managing access to and the protection of services and data that usually reside on hardware they don’t control.

Continued on [Page 8](#) »



Trust no users or devices, and always verify.

Migrate to a Zero Trust Architecture with Tanium to look beyond the users and data on your network and have full visibility into your devices.

[LEARN MORE](#)



INDUSTRY SPOTLIGHT

Shrink Your Security Blind Spots

Reduce complexity and improve security with data instrumentation at the edge

By Egon Rinderer, Global Vice President of Technology and Federal CTO, Tanium

Just as drivers have to contend with blind spots on the road, so do security practitioners and leaders defending their networks. And just as a driver's goal is to arrive safely at the destination, the objective of the chief information security officer is to ensure agency mission sustainment in a secure manner.

One of the biggest blind spots agencies have to contend with when securing their enterprise is rooted in data – how to instrument, move, store, analyze, distill and, most importantly, act on it. 2020 resulted in the transition to a majority remote workforce, making the data problem tougher to wrangle. While it was already difficult to achieve visibility and control of the devices that were within traditional agency network perimeters, that problem became significantly more complex as more devices moved off premises, and bring-your-own-device devices started accessing the network. Security blind spots multiplied.

Moving forward, federal agencies must work to eradicate these blind spots. How do agencies address the challenge?

1. Recognize a legacy approach:

Many agencies are struggling with a lack of visibility, but they're never going to be able to overcome the problem if they don't acknowledge it. Many of the past IT and security investments weren't inherently bad investments – they functioned as intended in on-prem environments. However, when the U.S. office workforce is more than 70% remote, that model and tooling is simply no longer a viable solution.

2. Instrument at the edge:

Agencies need to adjust the way they think about endpoint security. The problem isn't just about

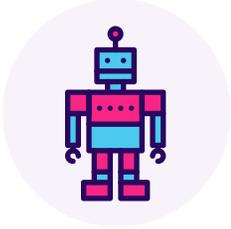
endpoints, it's about data. Data has three central tenets: velocity, variability, and veracity. Agencies have typically collected and centralized data – for storage, analysis and, eventually, action. But today, that type of approach either results in ineffective actions or total inaction, because the data is no longer useful. The value of data decreases with time, so when data is centralized, the ability to act on that data in a timely manner is lost. It's critical that agencies understand that centralized data collection is a legacy approach, and data instrumentation at the edge is the solution needed for enterprisewide real-time visibility and control.

3. Zero trust requires real-time data:

Many agencies are turning to a zero-trust model to better secure endpoints across a globally distributed workforce. However, no one solution collects all data and confirms or denies transactions in real time. Agencies need a method to bifurcate data instrumentation and collection. Instrumentation enables agencies to take action in real time. Collection allows for research and trends analysis. Agencies need to interact with data where it's produced – at endpoints. Data centralization isn't bad, but it should be reserved for only the most important data.

Many agencies think that to reduce security blind spots, they have to sacrifice the completeness, accuracy or timeliness of data. With legacy tooling, that logic is correct. With Tanium, however, there's no sacrifice required. Tanium's patented architecture allows federal customers to interact with data at the edge, leveraging every endpoint in unison as part of a real-time, living database. Data doesn't have to be moved and workloads can be distributed across every endpoint, allowing for a complete, accurate and real-time view of every endpoint on your network – and zero blind spots.

The Evil Axis's Arsenal



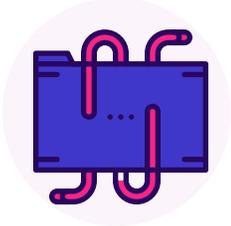
Bot: A type of software application or script that performs tasks on command, allowing an attacker to remotely take complete control of an affected computer. A collection of these infected computers is known as a “botnet” and is controlled by the “bot-herder.”



Phish: A technique used by hackers to obtain sensitive information. An example is a hand-crafted email message designed to trick people into divulging personal or confidential data, such as passwords and bank account information.



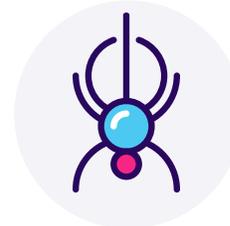
Ransomware: A form of malware that deliberately prevents you from accessing files on your computer, holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.



Exploit: A malicious application or script that can be used to take advantage of a computer's vulnerability.



Trojan Horse: A piece of malware that often allows a hacker to gain remote access to a computer through a “back door.”



Virus: A type of malware aimed to corrupt, erase or modify information on one computer before spreading to others. More recently, however, viruses like Stuxnet have caused physical damage.

Why should I care?

Having your identity stolen is seriously expensive and onerous.

You have to go through multiple government agencies, financial companies and personal services to get your life back together. And thieves could run up a check on your accounts in that time. Remember the Office of Personnel Management breach?

Cyber is part of your job.

Agencies try test-phishing campaigns against their own employees because they want to make sure they're ready for when the real thing comes. It's like a fire drill. Poor performance in cybersecurity could lead to reprimands or even termination. This is part of your job, and if you cost your agency thousands or millions of dollars, your career could be on the hook.

Cybersecurity is a priority.

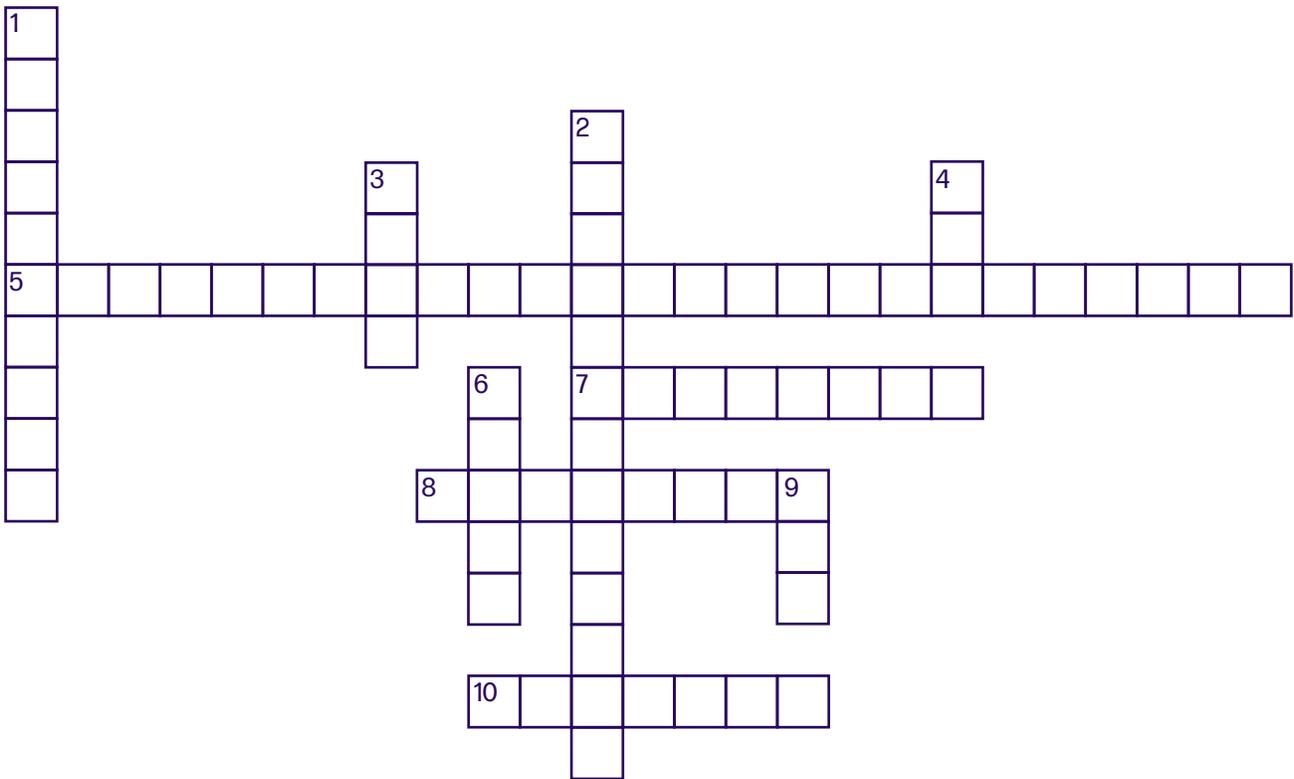
Agencies have identified cybersecurity as a priority, an order that has flowed down from the highest ranks. President Biden has singled out cybersecurity as an area for improvement, creating the new deputy national security adviser position that deals with cybersecurity and emerging technology. And after the SolarWinds hack, agencies are on high alert.

Attacks are on the rise.

Attackers have gotten better, and they're exploiting the COVID-19 pandemic to target individuals via phony emails and phone calls. The volume is higher in many sectors, and the attacks have become more targeted and sophisticated too. You could get caught slipping if you're not careful.

Crossword Puzzle

Answers are on [Page 43](#).



Down

1. A type of malware that encrypts and locks files
2. A particular type of cyberattack where a phony communication is disguised as from a known contact
3. Before you walk, _____
4. The federal agency charged with investigating and dealing with cyberattacks
6. Services accessed by the internet and stored off premises
9. Virtual private network, abbreviated

Across

5. A digital token often delivered by text, voicemail or email
7. L!r0ck\$t@R, for example
8. A centralized website for federal (and now some state and local) employees to log in
10. Keep all of your passwords in a password _____



New Workspaces + New Tools = New Risks

Work securely from anywhere
with modern authentication

Keep your workforce working securely from anywhere with modern, risk-based multi-factor authentication – including biometrics, passwordless and other methods that deliver the flexibility you need and the convenience your users want. SecurID™ gives you control across all access points, including supported and unsupported BYOD devices, wherever people work.

Modernize your approach to secure access
rsa.com/secuid



©2021 RSA Security LLC or its affiliates. All rights reserved. RSA, the RSA logo and SecurID are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries.

INDUSTRY SPOTLIGHT

How to Beat the Bad Password Blues

An interview with Steve Schmalz, Field CTO, RSA

Everyone knows that weak passwords are the scourge of strapping security. Unfortunately, strong passwords are not much better.

The problem is that strong passwords – say, those made up of 12 characters, including a mix of upper- and lower-case letters, numerals and special characters – are devilishly difficult to remember, so people come up with a way of making them simpler and, consequently, easier to crack. In any case, even the best passwords can be stolen.

That's why many agencies are turning to multifactor authentication (MFA), which requires not just a password – if one at all – but also a hardware or software token, a biometric (e.g., fingerprint) scan or other authenticators.

To learn more about multifactor authentication, GovLoop spoke with Steve Schmalz, Field Chief Technology Officer (CTO) at RSA, a provider of MFA and other cybersecurity solutions.

Schmalz highlighted three factors to consider when selecting an MFA solution.

Ease of Use

Ease of use is essential for MFA for a simple reason: If an authentication solution is too difficult, users will flood the help desk with trouble tickets or simply find a way to bypass the solution, Schmalz said.

Ease of use is equally important to administrators whose job it is to integrate the solution and keep it running. “If that's too complicated, then either they'll implement it incorrectly, or it just won't get implemented at all,” he said.

The net result? The organization will end up with passwords again.

Choice of Authenticators

When setting up an MFA system, an organization might be tempted to mandate a particular combination of authenticators, such as a password and smart card, for every use. The problem is that no authenticator is ideal for every use case.

For example, a smart card might work well for an end-user logging onto a laptop, but not so for a network administrator accessing a standard network router.

“If you have just one option, there are going to be situations where you can't implement it, and then you're back to password-based authentication as the only choice,” Schmalz said.

Risk-Based Governance

Typically, agencies see authentication – verifying a user's identity – as a separate function from verifying what resources they are allowed to access. But that shouldn't be the case, Schmalz said.

By unifying the two functions, an agency can take a risk-based process to protecting its resources. For example, the agency might want to require a higher level of authentication for a user accessing sensitive applications or data, or for users working from the road rather than the office.

RSA provides agencies with an MFA infrastructure flexible enough to develop strong authentication processes that work across a wide range of environments. As part of that, RSA has incorporated a cloud-based offering that works seamlessly across cloud-based, web-based and on-premises systems.

“By putting everything together, we're able to provide a portal to access all of the applications that you might need,” Schmalz said.

Passwords and Protections 101

“Open sesame! Abracadabra! Alohomora!”

Standard cybercriminal incantations shouldn't be enough to break your code. But when you set an easy password, with a standard phrase, no special characters and no backup checks, hackers can get in as easy as “1-2-3, open for me!”

Passwords are the front line of defense, the shield before the armor. In this section, we'll polish up your password strength and brush off misconceptions, adding a little glister to your cyber suit.

Quiz

Answers are on the following page. Source: [FTC](#)

1. Which of these passwords is the most secure?

- A. password
- B. Password1!
- C. P@\$\$w0rd!
- D. Grouchyc@tl@serPointer!

2. True or false: You should use the same password as much as possible so you don't forget your login.

3. Where is a good place to store your passwords?

- A. On a piece of paper
- B. In a password manager
- C. In a notes app
- D. All of the above

4. Which of the following does a password manager NOT do?

- A. Randomly generate tough-to-crack passwords
- B. Store passwords in a central database so that you can access them when you need
- C. Scroll through your existing passwords and tell you the ones that need work
- D. Ask for a master password to access your information

5. Which one of these statements is true?

- A. It's best to use multifactor authentication to access areas of the network with sensitive information.
- B. You should use the same password for key devices to guarantee that high-level employees can access them in an emergency.
- C. The best way to protect data is to make sure no one loses any device.
- D. You shouldn't limit login attempts on key devices, because getting locked out for having too many incorrect attempts would leave you unable to access your accounts.



Answer Key

1. **D.** The National Institute of Standards and Technology (NIST) recommends you create passphrases that are “easy to associate in your mind, are personal to you and preferably visual in some way,” such as “grouchy cat laser pointer.” These are easy for humans to remember and difficult for computers to guess. Always back them up with another layer of protection, like multifactor authentication, when possible.
2. **False.** If someone gets one of your codes, you don’t want them to get everything else. That’s not to say you can’t have favorites, but especially for important information, consider using unique combinations or a password manager.
3. **B.** You don’t want cybercriminals or brick-and-mortar criminals to pinch your information. So a notes app and notepad are both too susceptible to easy access. Use a password manager instead.
4. **C.** A password manager does a lot, but it’s up to you to determine the services you use and which existing passwords you have. It does, however, randomly generate complicated passwords and save them for the right website. All of that information is stored centrally, accessed with a master password.
5. **A.** Always use multifactor authentication to access areas of your network and devices with sensitive information. This requires additional steps beyond logging in with a password – like a temporary code on a smartphone, or a key that’s inserted into a computer.

The Elements of a Strong and Sturdy Password

North Dakota: “Passwords are keys; guard them like you guard your house key.”

Maricopa County: “Think of your password like your toothbrush: Change it regularly and don’t share it.”

So what makes a good password?

Maricopa County

- Passwords should be easy to remember, but hard to guess.
- Passwords should not be written down.
- Passwords should be at least eight characters long, containing mixed-case characters and special symbols or numbers.
- Passwords should not be easy-to-guess key sequences (e.g. “qwerty”).
- Passwords should not be dictionary words.



P Money
@Maechez1

I have no more passwords left in me

4:07 PM · Mar 24, 2021 · Twitter for iPhone

North Dakota

Our network and software security and firewalls can be the best and yet, if someone obtains our password, all the security in the world will not protect our data.

Do not include:

- Names
- Birthdates
- Seasons
- Hometowns
- Favorite team names, etc.

Hackers focus on the region of their potential victim, so they may try Fall2019, Vikings1, Packers1, Fargo2020, etc. as password attempts.

Continued on [Page 16](#) »



Security for Government, Everywhere You Need It

Federal, state, and local governments face rising cyber threats, tenuous budget forecasts, and the continuation of remote work.

Fortinet has the solutions agencies need to:

- Protect digital assets and critical infrastructure against advanced attacks
- Make the most of limited spending power
- Take advantage of key support programs and opportunities available from the Cares Act and the American Rescue Plan



INDUSTRY SPOTLIGHT

Telework Demands Secure Connections

An interview with Jim Richberg, CISO, Public Sector, Fortinet

Timing is everything. Imagine a global pandemic 10 years ago. Even then, such widespread telework wouldn't have been nearly as possible. And 20 years ago? Forget about it.

The move to large-scale remote work wasn't just about getting laptops to households. Rather, by 2020, network size, speed and availability had matured to a point where agencies – including some of the nation's largest employers – could reliably support their employees using wireless connections to reach the network. That left security playing catch-up.

“Serendipity played a role in success at doing remote telework – where many agencies were in their upgrade cycle and what technology choices they had made,” said Jim Richberg, CISO for Public Sector at Fortinet, a network security provider.

Agencies have succeeded thus far, but a digital world demands even more advanced network security structures. To progress, agencies can follow the below steps.

1. Recognize new patterns of work

2020 was “the year of the hybrid,” Richberg said.

The move to telework – portending shifts to longer-term hybrid environments – bore fascinating patterns, from shared school and work computer stations to work hours expanding beyond 9 to 5. These trends meant security teams had to re-evaluate red flags. Late-night logins and unrecognized activity used to be indicators of a breach; now, they blend into the work-life puree of every employee.

Another trend of note: Agencies everywhere opened up previously in-person jobs to geographically distant employees. Since employees didn't need to be office-bound, employers sourced from a broader pool of candidates. This was a major win for hiring teams, but blurred the important filter of location for network

security administrators, who previously marked an activity as suspicious if from an unrecognized location.

2. Understand faces on networks

Out-of-state employees aren't the only fresh faces on networks. Agencies have turned to robotic process automation – which has its own access credentials – to help handle the surge of citizen requests and resolve backlogs.

Security teams now must authorize and secure large numbers of connections to disparate internal databases. And as the digital surface grows, the threat landscape does too. Multi-vector, multi-impact, mixed “best of breed” attacks and AI-assisted targeting are becoming more commonplace.

Differentiating between legitimate and malicious network traffic will remain a challenge.

3. Roll out SD-WAN

Agencies can embrace the remote revolution by adopting a software-defined wide-area network (SD-WAN). SD-WAN reduces the cost and burden of providing remote workers with access to applications and data. And since security controls are integrated at the edge, traffic doesn't need to travel back to the data center, boosting the user experience.

Integrated security also improves visibility, helping administrators cut through the tangle of devices, accounts and profiles that clog up modern networks. Fortinet SD-WAN solutions also use automation to make connections simpler.

“The key should be spending smarter,” Richberg said. “And a key for governments is doubling down on upgrades such as SD-WAN, which saves money, increases staff efficiency, both IT and security, improves the user experience, and enhances security, productivity and resilience.”

How to Manage All of That

Here's where we run into trouble. We can follow these rules of thumb, and still stray from safety because we need so many passwords, with different requirements or different codes. So what do you do?

Password Manager: "Programs called password managers offer the option to create randomly generated passwords for all of your accounts. You then access those strong passwords with a master password." - Cybersecurity and Infrastructure Security Agency

What should you look for when seeking a password manager solution?

- **Lock-In Period:** Can you easily switch your information to another product if you don't like the first one?
- **MFA:** Does it support multifactor authentication?
- **Cross-Platform Capabilities:** Does it support each device platform you use?
- **Mobile Device Features:** What mobile device features does it have? For example, does it have biometric options instead of complicated passcodes?
- **Management:** Does it have a browser toolbar or menu to manage multiple saved accounts?
- **Autofill:** Will it autofill forms similar to your web browser?
- **Usability:** Is it easy to use?

What to Watch Out for

- Forgetting the master password - your account login info can be lost for good
- Password managers that don't automatically capture updated password events
- Logging in with your secure username and password to a website that doesn't use a secure HTTPS connection
- Default generated passwords that are not at least 20 characters long and include all of the major character types - uppercase, lowercase, numbers and symbols

Bonus Features: With advanced/premium options, it could:

- Manage passwords for applications
- Automate the password change process
- Securely share passwords with other users, preferably with advanced permissions, for when users are on a single or controlled account
- Offer large-scale secure storage
- Have built-in VPN

Source: Maricopa County



How long would it take for a high-powered server to guess these passwords?

- **Today123** - 36.99 minutes
- **Today1234!** - 19.24 years
- **Mi55ouriR!v3r** - 1.65 hundred thousand centuries

Source: North Dakota

Virtual Meeting Tips and Tricks

Be Mindful of Your Environment

Review your surroundings:

- Remove items with personally identifiable information (PII) from sight
- Keep in mind your camera view may change, so be aware of all your surroundings

Know of All Laws That May Be Applicable

- Make sure that your public video meeting complies with any legal requirements
- Be cognizant of any sort of notification and instructions you wish to share with participants

Security Is Key!

To reduce the risk of disruptive elements:

If possible ...

- Require attendees to register for the meeting
- Require them to authenticate before attending
- Password-protect your meeting

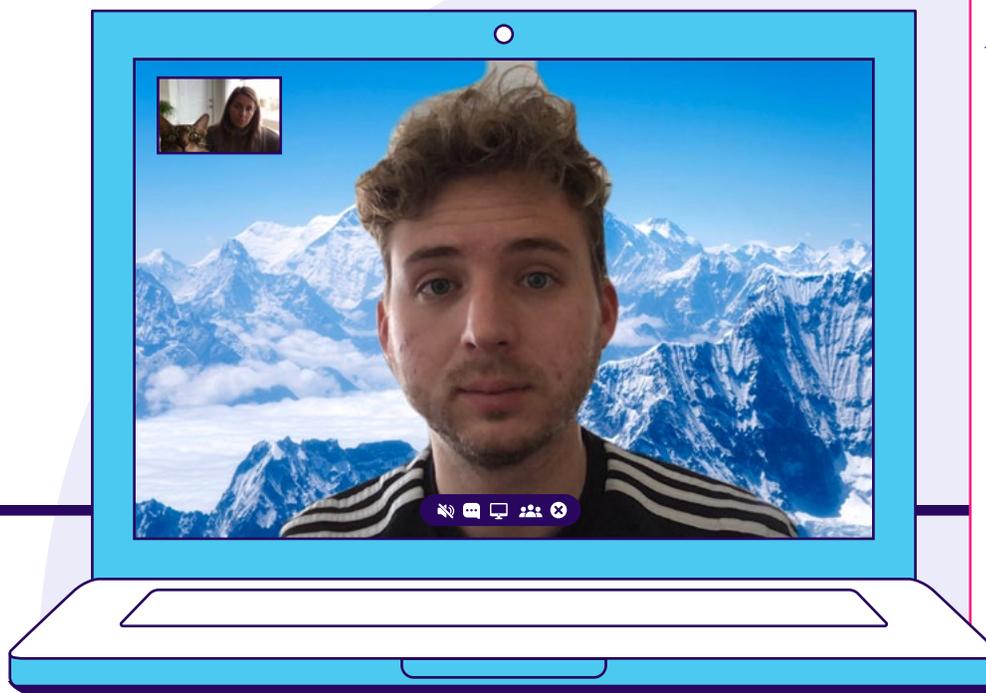
Double-check all your settings before hosting the meeting:

- Do not allow others to join a meeting before the host, in order to easily account for everyone participating
- Lock your meeting, if you can, after it has started so that people cannot join midstream and disrupt
- Unless needed, make sure participant screen-sharing is disabled
- Disable file-sharing to prohibit people from sharing inappropriate materials
- Have a moderator present who is responsible for maintaining order and removing disorderly attendees from the meeting

Privacy Concerns

- If you are going to record meetings, make sure you announce this fact to participants and remind everyone prior to the meeting start so they can opt out

Source: Maricopa County



◀ *Me, hosting a meeting from Mt. Everest, so that meeting attendees can't see any sensitive information in the background – or my pile of laundry.*

How to: On Zoom or similar platforms, hit the arrow within the "Start Video" button. Select "Choose Virtual Background," and either pick a preselected image, or add your own!



Akamai

Experience the Edge

IT Modernization Encourages Moving Your Critical Applications to the Cloud

The surge in your agency's remote workforce demands secure access and availability of those applications at all times.

A Zero Trust architecture ensures that when doing this, you trust but verify.

Learn more about how Akamai can partner with you on your journey to Zero Trust.

INDUSTRY SPOTLIGHT

The 3 Essentials of Remote Cybersecurity

An interview with Rob San Martin, Vice President of Public Sector, Akamai

The unforeseeable events of 2020, with unplanned, large-scale shifts to remote work, challenged how agencies manage their cybersecurity. As agencies pivoted, employees entered a “new normal” with heightened security measures that sometimes made it more difficult for them to access applications required to do their daily jobs.

Now, with remote work increasing the number of users and devices that must be protected outside their physical borders, it is crucial for agencies to revisit their cybersecurity methodologies and postures.

Going forward, government continuity and efficiently serving citizens depends on agencies’ security and operational effectiveness. For citizens, any obstacles they encounter in government systems can create frustrating delays for products and services like Medicare benefits.

Even worse, malicious actors are ready to pounce on any vulnerability. Today’s cybercriminals are more aggressive and creative than before.

“When your guard is down, you become an easier target,” said Rob San Martin, Vice President of Public Sector at Akamai, a leading cloud security and delivery provider.

With remote workers now relying more on the cloud for application and system access, agencies need a strong cybersecurity methodology to maintain stout defenses on and off premises.

San Martin shared three tips for robust security with cloud-based cyberdefenses:

1. Verify identities

For too long, agencies have trusted their users to be who they say they are. Going forward, San Martin recommended agencies exercise more skepticism when vetting users.

“It is irrelevant if it is a government employee, a constituent or a downstream contractor,” he said. “The identity of that person is the first step to avoiding these attacks.”

San Martin suggested agencies automatically distrust every user or device accessing their data, requiring their identity and permission levels to be verified each time they request access. This philosophy – zero-trust security – can keep cybercriminals away from their sensitive citizen data.

2. Monitor machines

Endpoints are remote computing devices such as laptops that connect to networks. As more agencies work remotely, the number of endpoints has increased dramatically.

“Everybody is starting to watch the machines,” San Martin said. “Is the machine acting like we anticipated, or does it need to be patched?”

3. Upgrade UX

Unfortunately, the more agencies scrutinize their devices and users, the more difficult work can become for their staff. Strict cybersecurity may keep data secure, but it can also become aggravating with multiple logins, authentications and passwords for employees.

Thankfully, cloud services like Akamai’s can help agencies implement zero-trust security without sacrificing quality user experience (UX). Cloud’s flexibility means it can easily support tools like secure login portals that employees can access and use with a single login. Furthermore, cloud can help agencies continuously monitor their networks’ devices and users.

“The overall solution gains strength, ubiquity and actual utility when the government starts to get comfortable with what that access solution is,” San Martin said. “But UX is what it all comes down to.”

Physical Security in the Digital Era

Government during the pandemic has transcended into the digital world. So thankfully, we really don't have to follow the same in-office safety protocols anymore, right? Actually, wrong.

In our new remote/hybrid state of work, physical security still matters – maybe more than before. Webcams and shared devices put your personal and work information in reach of outsiders. And as home and work lives blend, you're now the keymaster for your own privacy.



Quiz

Answers are on the following page. Source: [FTC](#)

1. Promoting physical securing includes protecting ...

- A. Only paper files
- B. Only paper files and any computer on which you store electronic copies of those files
- C. Only paper files, flash drives and point-of-sale devices
- D. All the above, plus any other device with sensitive information on it

2. True or false: Paper files that have sensitive information should be disposed of in a locked trash bin immediately.

3. True or false: When you hit the “delete” key, that means a file is automatically removed from your computer.

4. True or false: Only people with access to sensitive data need to be trained on the importance of the physical security of files and equipment.

5. True or false: Keeping your router’s default name will help security professionals identify it and, thus, help protect your network’s security.

6. True or false: Before connecting remotely to the agency network, your personal device should meet the same security requirements as agency-issued devices.

7. Which of the following describes the best way to make sure you are securely accessing the agency network remotely?

- A. Read your agency’s cybersecurity policies thoroughly
- B. Use VPN when connecting remotely to the agency network
- C. Use unique, complex network passwords and avoid unattended, open workstations
- D. All of the above

Answer Key

1. **D.** Promoting physical security includes protecting sensitive information in paper files and on hard drives, flash drives, laptops, point-of-sale devices and other equipment.
2. **False.** Always shred documents with sensitive information before throwing them away.
3. **False.** "Delete" alone does not actually remove a file from a computer. Use designated software to erase data, especially before you donate or discard old computers, mobile devices, digital copiers and drives.
4. **False.** Everyone needs to have strong physical security practices, and everyone should also be trained on what to do if equipment or paper files are lost or stolen, including whom to notify and what to do next. You can find more at [FTC.gov/DataBreach](https://www.ftc.gov/DataBreach).
5. **False.** Changing your router's default name and preset password can help protect your router from hackers.
6. **True.** When connecting remotely to the agency network, your device should meet the same security requirements as agency-issued devices that connect directly to the network.
7. **D.** Secure remote access requires all of these steps.

What's Wrong With This Image?

Something's going on here. Can you spot what's wrong?



Here's a freebie:

Change the default password on your home router. Cybercriminals are like car thieves, and default passwords are like unlocked cars. The better your unique password, the harder it will be for a criminal to break in.

There are six more problems.

Answers are on [Page 24](#).



Scale and Deliver Security Anywhere for your Remote Workforce With **Prisma™ Access**



paloaltonetworks.com/prisma/access

INDUSTRY SPOTLIGHT

Challenges for Security Personnel Have Grown: What They Need

An interview with MK Palmore, Field CISO for the Americas, Palo Alto Networks

In today's state of widespread remote work, the security landscape is seemingly easier for adversaries to exploit and tougher for security practitioners to protect.

With many employees in some posture of telework due to COVID-19, agencies face an exponential increase in viable targets that cyber assailants can successfully breach. In this evolving landscape, agencies need to reevaluate how to secure their employees' technology environment.

"Things have become more difficult for the security practitioner. But we do believe there is an answer to this," said MK Palmore, Field Chief Information Security Officer (CISO) for the Americas at Palo Alto Networks, a cybersecurity firm.

Security needs to be more seamlessly integrated to empower security teams and protect agencies in a changing environment. Here's how agencies can help their security personnel, according to Palmore:

1. Integrated security

Historically, security practitioners have used point solutions - addressing single use cases and created by individual vendors - to obtain best-in-breed cybersecurity. They have seeded these tools into their environment, assuming that a combination of tools yields the best security.

What Palmore and other experts have seen over time is that this approach does not produce the best security efficacy. As each year passes, successful and impactful breaches increase. As a result, agencies must explore critical security measures in a different way.

"We need to think about security as a more seamlessly integrated process, which provides security at all the points that would matter to security practitioners - network, cloud and endpoint," Palmore said.

A platform approach to security can provide a consistent strategy, where products are built together, work together and cover security needs from endpoints, to network and in the cloud.

2. Secure access service edge

A framework called secure access service edge (SASE), coined by Gartner, is an approach that meets agencies' evolving security requirements, particularly as more users need security in an increasingly connected and disparate IT ecosystem.

SASE can help by converging different security considerations into a more manageable environment for security personnel. It's a framework that best delivers enterprise-level security, because it allows users to access the assets they need and allows the organization to deliver security at the point of contact. This ensures security is able to scale to the needs of the enterprise user.

3. Automation

An ongoing shortage of trained and experienced cybersecurity personnel remains a major challenge. That's why automation is imperative.

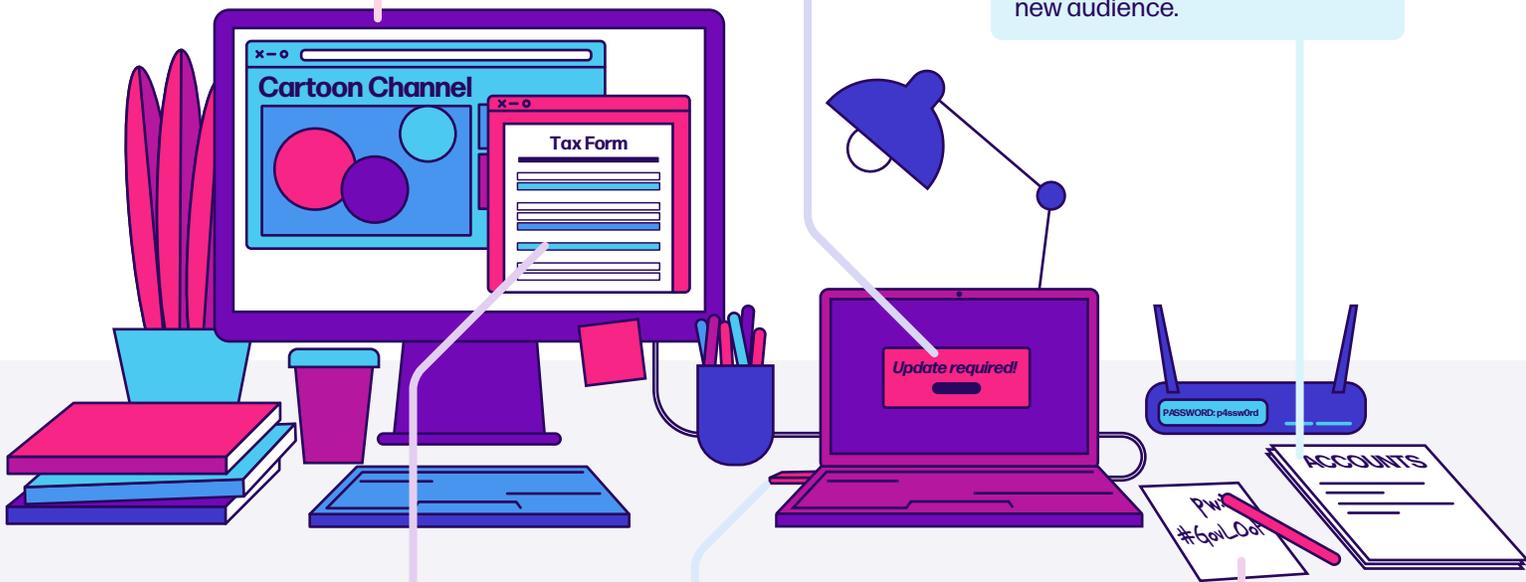
Automation of IT tasks and decision-making can augment and exponentially extend the productivity of existing security personnel by increasing the fidelity of alerts and contextualizing information. By the time an alert gets to security staff, automation contextualizes it in a way that allows the team to execute decisions quickly.

"Automation has now reached a maturity level that allows for organizations like Palo Alto Networks to build it into products and provide a game-changing way of tackling the needs of the enterprise," Palmore said. "It postures security analysts to now spend their valuable work hours addressing the most pressing needs."

Turn off or sleep your computer as soon as you're away from it. Even if you're at home, a house member or guest could see and use the information or accidentally share or capture it.

Set up auto updates to keep your computer's security software up to standard. Doing so means you'll receive patches to vulnerabilities as soon as they're available. If it's your work laptop, please ask your IT department first. They might want you to wait until they can vet the latest update.

Clear your desk of sensitive information. Even if no one in your immediate household poses a risk, webcams can bring your home life to a whole new audience.



Limit access to sensitive personal and work documents on your computer to just yourself. If you're relying on a personal device that the family has to use, make sure you connect securely, have antivirus protections and spam blockers, and close out all programs once done with them. You can even consider creating a separate computer account for work.

Double-check that this device is agency-approved. Otherwise, it should be nowhere near your laptop. Hackers can use flash drives and disks to install malware on your devices.

Never write down your passwords on paper. Rely on ones that you can keep in your head, or use a password manager instead.

Note: Install software and firmware updates on your router as soon as possible.

Cybercriminals are constantly looking for ways to take advantage of vulnerabilities (unsecure or weak programming) in your router. By updating your hardware as soon as new releases are available, you ensure you're one step ahead of villainy.

Summary: Secure Your Remote Workstation

- ✓ As we mentioned, use a strong password for your workstation and never share it. A strong passphrase (two or more words + numbers + symbols) is easy to remember but hard for a criminal to guess or crack. **If you have too many passwords to remember, try using a password vault. Not only can those store all your passwords, but password managers even create unique ones so you don't have to.**
- ✓ Just like with your router, **make sure you are updating your computer's operating system and computer hardware.** The newer versions of Apple and Windows offer automatic updates, giving you one less thing to keep on your to-do list.
- ✓ **Use multifactor authentication or two-factor authentication (2FA) everywhere it is offered.** Most banking apps and email providers offer one of these options, making sure that even if that super-secret password gets lost or stolen, the thief can't get to your sensitive information. For the best security, use an MFA/2FA app instead of text messaging or voice calling.
- ✓ **Lock before you walk.** The information on your workstation is for your eyes only. If you are using a personal computer for work, set it to auto-lock to ensure it will lock automatically if you forget to do it yourself before you walk away.
- ✓ You're not the only one who can get sick from a virus. **Your computer is at high risk of getting infected unless you use an antivirus program and keep it up to date.**
- ✓ If you are working with sensitive data that is covered by local or federal privacy laws, **make sure nobody else can see your screen or overhear your conversations.**
- ✓ **Turn on device encryption for your personal computer** to ensure that, if it gets stolen, nobody else can get to your sensitive information. MacOS users can turn on FileVault and Windows users can turn on BitLocker; both are available for free on newer versions.
- ✓ **Keep work life and personal life separate on your laptop.** Do not store work information on personal devices and vice versa. If at all possible, obtain a government-issued device to work from home. If one is not available, ensure your personal device is set up similar to how your work one is. Ask your tech support team for help.
- ✓ **Back up your important information.** If you are using a government-issued device, make sure you are saving all your work on a network folder or in a work-approved cloud storage area. If you are using a personal device, back up your personal information using a secure, password-protected cloud storage service (like Azure, Google Cloud, DropBox or others).
- ✓ Avoid using public Wi-Fi, but if you need to use it, **use a VPN connection** to prevent criminals from intercepting your internet traffic and stealing your information.

Source: Maricopa County

Just remember: PLUMBERS!

Wait, what?

PLUMBERS!

- P assword-protect accounts and devices
- L ock your workstation and screen
- U pdate operating systems
- M ultifactor-authenticate your accounts and info
- B ack up your info
- E ncrypt your personal computer
- R eport any attacks
- S eparate work and home lives

The background of the slide features a server rack on the right side, with a prominent red light indicator on one of the units. A thick white diagonal stripe runs from the top right towards the bottom left, crossing over the server rack. The left side of the slide has a light gray diamond-patterned background.

VERITAS™ | carahsoft®

Improve Resiliency in the Era of More

Address IT Complexity
with the most versatile
data protection platform
on the market

Learn more at www.veritas.com/resiliency

INDUSTRY SPOTLIGHT

Building Your Security for the Modern Era

An interview with Bryan Jenkins, Director of Sales, Carahsoft

The pandemic summoned a state of uncertainty about all we know, from street interactions to work attire. No one was happy to see the chaos - well, except cyberattackers, who seized on the lack of visibility to crawl into personal and business information.

Feasting on disorder, hackers sprayed COVID-19-themed phishing attempts. You know the ones, falsely promising “vaccine appointments” or fearmongering from a fake World Health Organization.

Cybercriminals’ goal is to turn panic into profit. Agencies’ and individuals’ responsibility is to stop them.

“If you’re not staying vigilant and staying in front of the threat in terms of training, then you’re behind the eight ball already,” said Bryan Jenkins, Director of Sales for Carahsoft. “You have to always be looking for what the next threats are, making sure your employees are up to date.”

Carahsoft, a prominent technology distributor, enrolled its employees in a new serial cybersecurity training during the pandemic. It catered toward telework security events, with the focus of continued improvement.

Though agencies are at different levels of cybersecurity, step No. 1 is educating and informing. Then, it falls on technology.

Step 1: Educate

Many agencies have been sticking with the same cybersecurity training since they sent employees home. But much of that training no longer applies. Water cooler chats are so 2019.

Cybersecurity training should be centered on modern events - situations employees connect with, like spear phishing or suspicious links. As employees beef up their knowledge, agencies progress to a secure, long-term remote and hybrid environment.

Step 2: Secure

Much of security is focused on preserving operations, though that’s not always what hackers want to topple.

If intruders can make off with agency secrets or sensitive information for the black market, their payday is complete. Where they often exploit this information is backups, which can be forgotten in agencies’ rush to lock up everything else. Given these contain years of sensitive information, backups are a prized pinch for attackers.

“That’s probably the biggest piece of the pie attackers are going after,” Jenkins said.

In a backup and recovery solution, agencies should look for encryption capabilities. They have to be able to restore that information from a secure place off premises.

Step 3: See

One reason why many agencies leave sensitive data exposed is they don’t know where it is. In some cases, hackers will stumble upon it before IT does.

With the amount of novel data only growing, few agencies have the resources to take stock of all their archives and backups. So what should they prioritize?

One answer comes via Carahsoft’s partnership with Veritas, a data specialist. The tool combs through documents to identify sensitive information, like passwords or personally identifiable information. It can also find “orphaned” files without an owner.

This sort of visibility and understanding is a crucial pillar of a backup and recovery strategy geared toward the ransomware era.

“In a ransomware-type scenario, you want to obviously protect the most sensitive information the most, because that’s what the bad guys are going after,” Jenkins said.

Phishing, Ransomware and Common Threats

It used to be that fraudulent emails came from criminals masquerading as deposed princes of Fairytaleland who, as requested in broken text, needed \$10,000 to reclaim their crown. No longer!

Cybercriminals have gotten smarter. The emails look more legitimate, sometimes even with the logo of a company you use or with a name you might recognize. Usually, they're not even asking for your credit card number straight away.

So how can you be sure to spot a phishing attempt? And what should you do with one?

Keep reading.

Quiz

1. Which one of these statements is correct?

- A. If you get an email that looks like it's from someone you know, you can click on any link as long as you have a spam blocker and anti-virus protection.
- B. You can trust an email really comes from a client if it uses the client's logo and contains at least one fact about the client that you know to be true.
- C. If you get a message from a colleague who needs your network password, you should never give it out, unless the colleague says it's an emergency.
- D. If you get an email from human resources asking you to provide personal information right away, you should check it out first to make sure they are who they say they are.

2. You get a text message from a vendor who asks you to click on a link to renew your password so that you can log in to its website. You should:

- A. Reply to the text to confirm that you really need to renew your password
- B. Pick up the phone and call the vendor, using a phone number you know to be correct, to confirm that the request is real
- C. Click on the link, and if it takes you to the vendor's website, then you'll know it's not a scam
- D. All of the above

3. True or false: Email authentication can help protect against phishing attacks.

4. If you fall for a phishing scam, what should you do to limit the damage?

- A. Delete the phishing email
- B. Unplug the computer to get rid of any malware
- C. Change any compromised passwords
- D. All of the above

5. What is ransomware?

- A. Software that infects computer networks and mobile devices to hold your data hostage until you send the attackers money
- B. Computer equipment that criminals steal from you and won't return until you pay them
- C. Software used to protect your computer or mobile devices from harmful viruses
- D. A form of cryptocurrency

6. Which of these best describes how criminals start ransomware attacks?

- A. Sending a scam email with links or attachments that put your data and network at risk
- B. Getting into your server through vulnerabilities and installing malware
- C. Using infected websites that automatically download malicious software to your computer or mobile device
- D. All of the above

7. True or false: If you encounter a ransomware attack, the first thing you should do is pay the ransom.

8. An email from your boss asks for the name, addresses and Social Security numbers in a tax agency's system. The email says it's urgent and asks you to please reply right away. Should you go along with the request?

9. True or false: Local backup files – saved on your computer – will protect your data from being lost in a ransomware attack.

10. True or false: Updating your software as soon as possible is one of the best ways to protect from ransomware.

Answer Key

1. **D.** This email could be a phishing scam, in which you get a message that looks like it's from someone you know, asking you to urgently provide sensitive information. Never give up your information without confirmation of their identity. Your spam blocker and software might not prevent everything, and you should never give up information so readily, even to a colleague.
2. **B.** Before you click the link, make sure the text is legitimate and the request is real. Otherwise, clicking on the link could download malware or expose company credentials.
3. **True.** Email authentication technology helps prevent phishing emails from reaching your inbox.
4. **C.** If you fall for a phishing scheme, you should immediately change any compromised passwords and disconnect any computer or device that could be infected with malware from the network. This will help limit the damage. Then, look into other steps, such as who to report the attack to.
5. **A.** Ransomware can be delivered many ways, but it's always software that infects computer networks and mobile devices to hold your data hostage until you send the attackers money.
6. **D.** Criminals can send a scam email with links or attachments, get into your servers or disperse malicious software through infected websites to append ransomware onto your computer.
7. **False.** First, disconnect the infected computer or device from your network. If your data has been stolen, take steps to protect your agency and notify those who might be affected. Check to see if you can restore your systems from backups. Then, determine whether to pay the ransom, knowing that law enforcement doesn't recommend it and that paying the ransom doesn't guarantee you'll get your data back. Be sure to report the attack to proper authorities, per agency guidance.
8. **No.** It may be a phishing attempt, given the signs. Call your boss and confirm whether the request really did come from them. Also, look for common indicators of a phishing attempt, such as a misspelling or vague requests for information.
9. **False.** Once hackers have access to your computer, they can find ways to steal additional files. Important files should be regularly backed up on a drive or server that's not connected to your network. Be wary, because hackers can still steal sensitive information in this case.
10. **True.** Fixing your settings to update automatically can help you make sure you're working with the latest and greatest security on your personal computer. At work, check with IT to see if you should do the same, because the department might also send out software updates on its time. On mobile devices, you may have to update manually.



We know the landscape, and how to innovate in it

Modern security means shifting from a strategy of minimizing change to one that is optimized for change.

www.redhat.com/gov



INDUSTRY SPOTLIGHT

Dealing With Complexity in a Tangled World

An interview with Michael Epley, Chief Architect and Security Strategist, North America Public Sector, Red Hat

Technological advances have driven the workforce and humanity to new heights, even enabling a society that functions largely digitally during a pandemic. But the proliferation of applications, accounts and the like creates new challenges for security – a more-tech-means-more-problems conundrum.

Unmistakably, technology has become more complex. Instead of one smart device, you likely have several. Instead of one password, you probably have an array. Instead of one login screen, you often have to go through multiple gates.

Security is scrambling to keep pace in the innovation race, and try as it may, it often strays behind. There's just so much to secure, and with the infamous cyber skills shortage in government, teams don't have enough hands for it all.

"There's a tremendous amount of complexity involved here," Michael Epley, Chief Architect and Security Strategist for Red Hat's North America Public Sector. "It's very difficult to get people that can look at all those different systems and integrate, or tie them all together, safely."

But security isn't locked into a losing battle; it can still catch up.

Relearn the practice

Imagine someone strolling through an apartment lobby and pressing on door handles until they find an unlocked room to ransack. That's what hackers try inside networks.

To make it more difficult, agencies need constant security checks – at the front door, in the elevator and for each individual room.

Zero standing privileges is a concept that prevents guaranteed entry. It's an extension of the least-privilege model and paves the way for a zero-trust security strategy, which constantly asks users to verify identity.

Layered on top, privilege access management ensures on-demand access for users after they prove they need it. Criminals are locked out, and users can access the room they need.

Verify identity

Having more locks makes no difference if one key opens them all. In other words, users need more than one way to verify their identity.

Identity checks now rely on multifactor authentication, an example being a texted code. The problem here is that employees don't want to be treated as strangers in their own agencies.

An easy way for agencies to maintain security without encumbering employees is biometric authentication, like fingerprint and facial ID, Epley said. These secure and easy-to-use MFAs don't impede productivity and promote acceptance, not circumvention.

Don't go alone

Agencies need data from all their services working together to beat back attacks, but integration is no small feat. For that reason, many are looking for ways to manage the complexity of securing their enterprises.

Turning to managed security services is one strategy facilitated by cloud platforms. Managed services essentially outsource security – as completely or partially as agencies would like in areas like zero trust – while still giving agencies control of their data and policies. Combined with clearinghouses for intra-agency risk and threat analysis, these services respond quickly to their environments.

"You're using a managed service that's presumably provided by an expert in that particular piece of technology. That's why you're starting to see a rise of more managed services," Epley said.

Catch a Phish(ing Attempt)!

These emails are a little phishy.

Sometimes, you can tell from the address alone what's going on. The jig is up right here. Why would the official company have an odd address with numbers like this one? Still, keep reading.

From: cloudservicesteam45@gmail.com

Subject: Your Account Info

Hi Friend,

We've noticed some unrecognized activity going on on your Web Client account.

As a result, we've locked your account.

To open it up, you'll need to provide us with your account information and proof of identification. It's an easy process; just respond to this email.

- Your Cloud Services Provider

Be wary of emails that target account information. To check if they're real, don't be afraid to independently look up the company phone number and ask if this email is from them.

Notice the generic opening. That's unusual for a company with your information. This could be so that they can send the same email to lots of addresses.

Odd capitalizations and phrasings can be a dead giveaway. At big companies with large marketing departments, mistakes wouldn't get by.

Is your account actually locked? Don't be afraid to close the email and go to the page you have gone to before to log in.

This information is almost never solicited by email from reputable sources. Safe to say, you should forward this to your security team and delete it from your inbox.

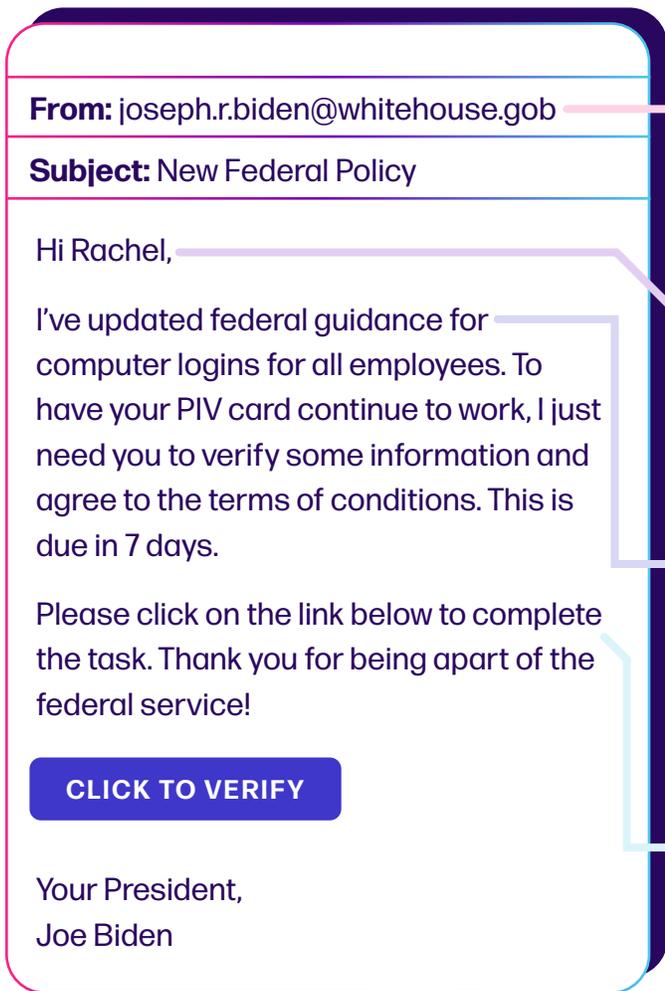
NEVER:

- ✗ Respond with information
- ✗ Click on links
- ✗ Download attachments
- ✗ Share with colleagues outside of IT

ALWAYS:

- ✓ Avoid any links or attachments
- ✓ Report to proper channel
- ✓ Inform others who may have been exposed
- ✓ Delete the email





This email address has the guise of authenticity until you see the last letter. Be careful; cybercriminals can be tricky. Even if the email had a .gov address, beware of such a request for sensitive information in an unexpected manner.

This email is shaping up to be a spear phishing attempt. That means it's supposed to rely on a recognizable connection to create a false sense of trust.

Does this sound right? Why haven't you heard of this policy elsewhere? Something's wrong. Ask around the office and to your supervisor, who would have been in on this information.

This email seems suspicious enough. Don't click on the link. Forward to IT to see what they find out about it. You might even prevent another user from falling for the trap!

What if you fell for a phishing attempt?

If they stole some of your information: Don't panic, but act quickly. Go to IdentityTheft.gov if they have your information, and report the attempt to your IT department if it's at work. Also, let the FBI [know](#).

If they stole some of the agency's information: Report it immediately to the IT team. Time is of the essence. Change the passwords for any personal accounts that you might have given them access to. If you're able, encrypt information you're sending over.

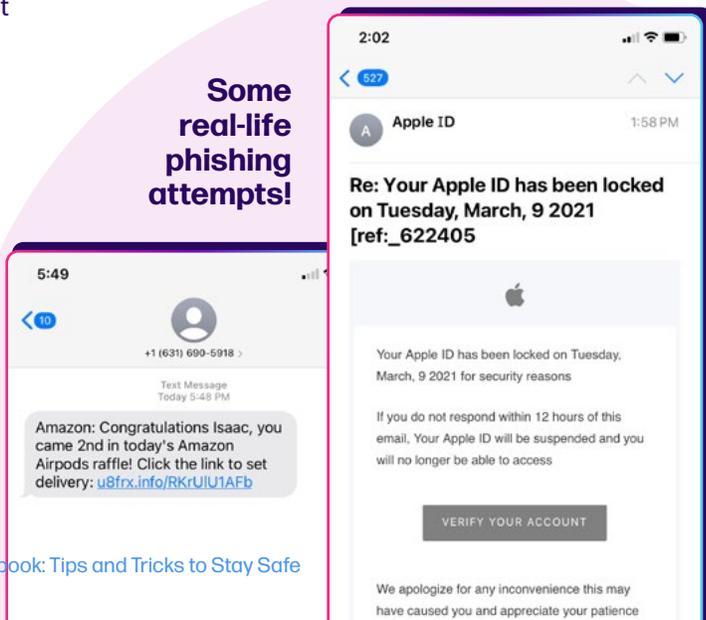
Phishbusters

If there's something strange in your inbox, who you gonna call?

F-B-I!

Want to really save the day?

Report if an attack is going around your community. You can report phishing in your private or professional life to the FBI [here](#), and at work, always let your IT team know. The FTC also has an [online portal](#) to report fraud and scam phishing attempts in your area. That information is then passed along to local law enforcement.



Some real-life phishing attempts!



Secure by Design

Leading the way to safer IT

solarwinds.com/secure-by-design-resources



Scalable, end-to-end IT monitoring software from solarwinds.com/government



INDUSTRY SPOTLIGHT

How We Can Get Through Today's Cyberthreats Together

An interview with Brandon Shopp, Vice President of Product, SolarWinds

There's no escaping that COVID-19 has been an especially devastating and dangerous time for cyberattacks. Attacks have shelled agencies, and though some have been in the news, others have gone largely unnoticed.

Cyberattacks are somewhat taboo in IT circles. No one wants to admit when they've been compromised or made a mistake, even though communicating early is the most surefire way to prevent major data loss.

"What I share today could stop the next attack happening to another agency tomorrow," said Brandon Shopp, Vice President of Product at SolarWinds.

One challenge for agencies is the lack of transparency around their cyber ecosystem. Because infrastructure is off premises, in the cloud, and employees are off premises working from home, agencies are relying on self-reporting that may not come soon enough.

Stopping cyberattacks is going to take all sides working together: individuals, agencies and industry. A three-pronged approach can accomplish this feat.

1. Understand

COVID-19 sent tremors down the spines of organizations, shaking up everything from workflows to routines. And as the permanent impacts of the pandemic have become increasingly clear, agencies should shed the security of the past.

In remote environments, cloud solutions are in vogue. After initial training, security teams should communicate to employees what the cloud means for them. Agencies should also explore solutions designed for a hybrid and remote world, such as endpoint detection and response software, which discovers and assigns security controls to devices on the network.

2. Educate

Education should take center stage – for everybody.

Employees need to understand working remotely requires more mindfulness, not less. "If you see something, say something," Shopp advised, and check in on security best practices in your home and work lives. Agencies can also beef up their knowledge of cloud-based apps and services. These off-premises offerings come with various amounts of security attached, but agencies are still responsible for their data.

Vendors need to carefully walk agencies through contracts and policies, and they should be available for questions. Part of their responsibility is putting supply chains and terms and conditions out front.

3. Share

If these seem like murky and uncharted waters, well, they are. Now isn't the time for finger-pointing but shared cyber growth.

Continuing its efforts in the wake of the breach, SolarWinds is working to foster information-sharing networks and free spaces for employees, agencies and organizations to ask cybersecurity questions without judgment. In these spaces, cybersecurity experts come together to share best practices and answer questions both simple and complex. The advice is priceless.

Information sharing and analysis centers (ISACs) have been sources of major assistance within the IT space, though many are siloed. The Multi-State-ISAC and IT-ISAC are two proven leaders that have shared best practices for years, a model everyone can follow.

"We need to break down those silos and truly make it a cyber community and not a set of cyber verticals," Shopp said.

Cybersecurity Spotlight: Login.Gov

This article has been republished with the permission of the author.

By Bill Hunt

In February 2021, the [General Services Administration \(GSA\)](#) announced that Login.gov is available for use by local and state governments. This is the biggest govttech news in the last five years.

Login.gov is a GSA solution to help solve the difficult problem of verifying that a person is who they say they are to receive a government benefit, as well as a solution for logging into government websites. It was created through the combined efforts of the United States Digital Service (USDS) and 18F – the two most prominent digital service teams in government – and is in use by many federal agencies. Today, it provides access to government services for **over 27 million people**.

Moreover, as [I've written in the past](#), it is my hope that the Office of Management and Budget (OMB) will **mandate** the use of Login for all federal agencies. This is [already mandated by law](#), but OMB is not enforcing the requirement. The most expensive part of the tool is the identity verification step. However, once an identity has been proven, it does not need to be re-proven if the customer wants to use any other service that is using Login.

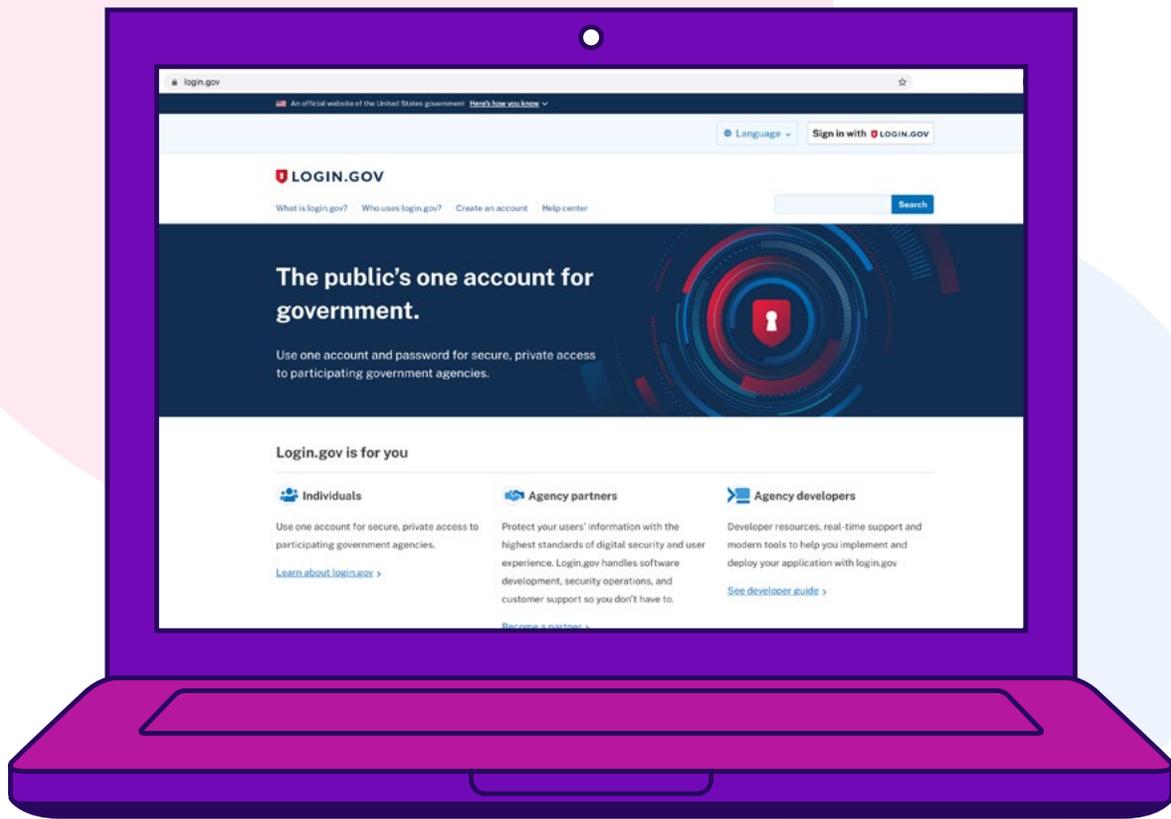
This means that as more organizations sign up for Login, the cost to each decreases. By allowing federal agencies to maintain their own independent login systems, the costs remain high. Moreover, this presents customers with an inferior experience, as they must sign up for a new account for each website or application.

It's also important to note that most identity verification behind the scenes is using data sources that the government controls and gives to private companies, which then sell the government back its own data in the verification process at a very high premium. Eventually, it would be smarter to allow agencies to exchange the necessary information themselves, cutting out the middle person, which would decrease the cost to *almost nothing*. (Congress, of course, could speed this along too with the right legislation.)

The Login team has also been working on a pilot to allow customers to prove their identity in person at a government facility, which has shown to improve the success rates of the verification process. The Veterans Affairs Department (VA) uses such a process to help veterans set up their online accounts right in the lobby of VA health clinics.

The U.S. Postal Service also performed a similar pilot several years ago, where anyone could stop by a post office and have them review their documents, or even let their postal carrier perform the review when they drop off the day's mail, allowing them to reach almost every single person in the country.

Detractors still complain about the cost of Login.gov and consider that a reason to not require it – even though the cost would be reduced if it was mandated. Even so, if the federal government agrees that this is the tool that agencies should be using, then it should be treated as a public good, like a library or park. To that end, Congress could pass appropriations dedicated to funding this critical program, for instance, as part of [President Biden's proposal for Technology Transformation Services funding](#).



However, I would caution agencies from implementing identity requirements **beyond what is absolutely necessary!** The [Digital Identity Guidelines](#) from the National Institute of Standards and Technology are the baseline that most federal agencies use. In my personal opinion, they set too high a bar.

The government must provide critical services to at-risk and economically disadvantaged groups. By setting requirements that individuals in these groups cannot meet, agencies are not serving people equitably. For instance, the VA serves veterans who may be experiencing homelessness, may not have a credit card, may be partially or fully blind, may have trouble remembering or recalling information, may not have fingerprints, and so on. Because the standard methods of identity verification and authentication may present an impossible barrier for the very people the VA serves, it is in the best interest of these people to not implement NIST's high standards as written.

There are, however, still a few restrictions for city and state use of Login.gov. To be eligible, the government agencies must be using Login for a "federally funded program." I am hopeful that this restriction will be removed in the future and this incredible service will be open to all who want it.

If you're a city or state government interested in a world-class identity solution, I'd recommend reaching out to GSA about Login.gov! Even if you don't meet this requirement, it's definitely worthwhile to get in touch with GSA anyway. As we've learned, policies change every day.

Bill Hunt is a technology-policy enthusiast who currently works for the U.S. government. Previously, he spent 20 years building award-winning software and teams in the private sector. His article was originally posted on billhunt.dev.

SECURE PRIVILEGE. STOP ATTACKS.

ACROSS THE ENTERPRISE · IN THE CLOUD · ON ENDPOINTS

Unsecured privileged accounts add risk to your business anywhere they exist - 100% of advanced cyber attacks involve them. Seamlessly protect privileged accounts across the enterprise - on premises, in the cloud and on your endpoints with CyberArk.

Federal Certifications and Compliances Include:

- DoD UC APL
- Common Criteria Certified
- NIST SP 800-53 / -171 / -82 / -63
- NERC-CIP
- DHS CDM Phase II Privilege Management Solution
- Army Certificate of Networkiness (CoN)
- Available on DoD Cyber Range
- HSPD-12
- FIPS 140-2
- NIAP certified

Learn about our Federal capabilities at:

CyberArk.com

©2020 CyberArk Software Ltd. All rights reserved.



INDUSTRY SPOTLIGHT

The Foundation for Future-Facing Cybersecurity

An interview with Kevin Jermyn, Federal Customer Success Manager, CyberArk

Cybersecurity has begun a new chapter, and it's time for agencies to flip the page. The old moat-and-gate model is antiquated, but still, many agencies operate with the assumption that their attackers are on the outside looking in.

Unfortunately, bad actors are likely on the inside of agency networks and systems right now, and if not, they will be soon. How far they go, and how much damage they do, is determined by security structures.

"While cyberattacks are inevitable, negative business impact is not," said Kevin Jermyn, Federal Customer Success Manager at CyberArk, which specializes in identity security.

Those clinging to the vestiges of rotting security structures could meet nightmarish attacks. But those willing to transition to modern models that recognize attacks past the surface can protect their assets.

In a few easy motions, agencies can begin that transition.

1. Assume breach

Agencies must begin with an "assume breach" mindset. Simple identity safeguards, like locking accounts after too many password attempts, aren't enough.

During the SolarWinds breach, purportedly the work of nation-state actors, attackers worked methodically and sophisticatedly so as not to trip any wires or raise any red flags. These kinds of attackers are well-equipped and don't act carelessly in search of a quick payout.

To frustrate hackers and make them resort to desperate approaches, agencies can employ privilege. With least privilege, employees can only access network resources if they're essential to their job. One-off permissions are handled ad-hoc.

"Implementing preventative controls that consistently enforce least privilege will help buy an organization invaluable time," Jermyn said.

2. Promote transparency

The first step to stopping a breach is spotting an attack. The next is reporting it.

But when it comes to communication, cybersecurity is sadly an area clouded with secrecy. Often, no one wants to report an attack, afraid of being the messenger. But in the hiatus between first signs and first report, the attack snakes across systems, inflicting all the more damage.

Agencies need greater cooperation and transparency from all parties. Employees should have a clear reporting pipeline for when they notice something amiss, and they need to feel secure doing so – possibly pointing to confidential disclosure. For vendors, government can ensure specific items for cybersecurity action and transparency, like confidential reporting, are a part of every contract.

3. Prioritize identity

All signs point to identity as the future of cybersecurity. Identity-centric security works off the principle of least privilege for access management and secures both human and machine entities.

A leader in privileged access management, CyberArk uses AI to eliminate friction and provide a seamless end user experience. Real-time analytics and processing can quickly detect suspicious behavior to snuff out cyberattacks.

Identity covers three main areas: authentication, authorization and auditing. In order, it processes credentials, proves identity and creates a paper trail of behavior. That means agencies can stop hackers in their tracks and trace back their steps to shore up the enterprise.

"Identity security accelerates business agility, while giving agencies the peace of mind that their crown jewels will be shielded from attacks," Jermyn said.

Logging Off: Tips for Securing Your Work and Your Family

Never leave your device where it can be stolen.

Ensure your office and home are locked, and never leave your mobile devices in your car or in a public area unattended.

Enable Find My Device and Remote Wipe on your mobile phone, laptop and tablet.

If you lose your device, you can use the Find My Device feature to locate it as long as it is still powered on. If your device is stolen, use the Find My Device feature and notify your local police department. If you're unable to retrieve your lost or stolen device, use the remote wipe feature to ensure your information is not stolen. If you are using a government-issued device, notify your tech support team immediately.

Be extra aware of email phishing and scams.

Cybercrime is at a record high because employees are less likely to practice good cybersecurity practices when they're not in a formal office setting. If an email looks suspicious, report it to your tech support team. Be careful when opening attachments or clicking on links.

Be cautious of what you post on social media.

Cybercriminals are perusing the internet looking for information about you. Avoid posting about leaving for a vacation and be wary of those personality quizzes. Many of them ask the same kinds of questions that can be used to guess or retrieve your passwords.

Check to see if your accounts have been breached.

With the number of data breaches on the rise, the chances of your personal information being available to criminals is high.

Keep a separate email account for junk and spam mail.

This is the account you can use to sign up for special offers, rebate/loyalty programs and all the other places that insist on filling your inbox with marketing material. Your real email account should be used to communicate with the people you trust.

Never use your work email for personal reasons and vice versa.

As a government employee, all of your work communication can be made public through public records requests or court orders. You definitely don't want your personal email messages to go public.

Manage your passwords, and don't let your passwords manage you.

Your life will be much the easier if you learn how to craft strong, reliable passwords and use a password manager. Always seal in the password with an extra stamp of multifactor authentication.

Source: Maricopa County



ivanti

[Learn More](#)

INDUSTRY SPOTLIGHT

A Clarion Call: Kill the Password

An interview with Bill Harrod, Public Sector Vice President, Ivanti

Cumbersome and ineffective password requirements beg the question: Is there a better way? The answer is certainly yes.

The federal government already relies on personal identity verification (PIV) cards as the first identity check at the door, literally. These cards are used to access federally controlled facilities and log on to agency information systems. With modern endpoints and mobile devices, relying entirely on a PIV card reader is not practical. Using another authentication factor, like biometrics using facial recognition or fingerprints, provides a more secure and user-friendly method to authenticate identity.

But even with appealing alternatives, passwords continue to be used to access applications, creating frustration for employees and an easy threat vector for adversaries.

“We have the solution to kill the password, and go to zero sign-on,” said Bill Harrod, Public Sector Vice President for Ivanti.

Agencies need to hear the clarion call. Cybersecurity is better when employees are on board with the plan. Step one is a smoother log-on.

Kill the password

No one loves passwords. For years, passwords have been the most easily compromised security control, even with more stringent and complex composition requirements, Harrod said. Additionally, a recent Ivanti survey found that a quarter of employees use the same password for their work email and commercial accounts.

That’s a major problem. Using work emails for online apps gives additional information to hackers trying to gain access. And with derived intelligence from

social media and other online sources, credential compromises and increased phishing attacks are all the more likely.

Correcting this behavior should be a priority, but agencies should also focus on changing the method of authentication, especially for cloud-based apps and government-protected resources. Shifting away from passwords can be a significant benefit to agencies’ security posture while improving employee privacy protection, as well.

More edge security where users are

Biometrics are one way to leave passwords behind, and they’re well-suited to telework. Many mobile devices – from phones to laptops – already have biometric features, such as facial and fingerprint recognition. Those generate an authentication token sent to the network that verifies identity and permits access. Digital credentials derived from PIV cards and accessed only via biometrics serve as a strong, password-free multifactor authentication.

Agencies can also implement per-application VPNs. These VPNs send traffic straight to the cloud for each application. The route cuts out circuitous traffic, meaning faster connection times and streamlined service for users. It also boosts security, with more frequent access authentications.

Partners like Ivanti can help here, applying application-level security and PIV-derived credentials, and validating identity and connections seamlessly on external endpoints.

“There really is a better together story,” Harrod said.

Conclusion

Well, there you have it. Sadly, we've reached the end of our cybersecurity guide.

It's reassuring to know that as complicated as this all can be, you don't have to understand the ins and outs of cybersecurity to keep yourself and your agency safe. Keep these best practices in mind, and feel free to quiz yourself again or complete the crossword puzzle to see how up to date you are.

With that, it's time to sign off and sign up for a password manager.

About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | [@govloop](https://twitter.com/govloop)

Thank You

Thank you to Akamai, Carahsoft, CyberArk, Fortinet, Ivanti, Palo Alto Networks, Red Hat, RSA, Solarwinds, Tanium and Veritas for their support of this valuable resource for public sector professionals.

Author

Isaac Constans, Senior Staff Writer

Designer

Kaitlyn Baker, Creative Manager

Crossword Answers

Down

1. Ransomware
2. Spear Phishing
3. Lock
4. FBI
6. Cloud
9. VPN

Across

5. Multifactor Authentication
7. Password
8. Login.gov
10. Manager



1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com

[@GovLoop](#)

