

JOURNAL OF

Civil DEFENSE

VOLUME 60

2025 ISSUE 1

AMERICA'S NEXT WAR: CYBERSPACE

www.TACDA.org

Photo by Philipp Katzenberger on Unsplash

TACDA™ is a registered 501(c)3 non-profit, non-political organization.
Donations are always appreciated.

Together We Are Stronger. Let Your Voice Be Heard!

Contact your elected officials! Tell them your emphatic desire to have an official Civil Defense Program for our citizens, no matter the cost.

Our United States government currently:

- Has NO Department of Civil Defense
- Does NOT educate our children about the effects of nuclear weapons
- Has NO fallout shelters for the general public
- Has NO directives on how to build hardened fallout shelters
- Has NO information for post-war survival
- Has NO government directed warning systems, sirens, evacuation plans, or general preparations for nuclear attack available for the general public

Here are three easy ways to find and contact your Senators:

1. By Email

Go to <https://www.senate.gov/general/contacting.htm>, locate your state's senators with the provided links, and email them.

2. By Telephone

Call the United States Capitol Switchboard at (202) 224-3121.

3. By Postal Mail

You can direct postal correspondence to your senator or to other U.S. Senate offices at the following address:

For Correspondence to U.S. Senators:

Office of Senator (Name)
United States Senate
Washington, D.C. 20510

For Correspondence to Senate Committees:

(Name of Committee)
United States Senate
Washington, D.C. 20510

Click [here](#) or scan the qr code to contact the United States Senate.



IN THIS ISSUE

- 4 The Importance of Cyber Security for Protecting Critical Infrastructure in America**
By TACDA Staff - AI Assisted
- 7 Risks of Smart Home Gadgets**
By Bryson Meiling, MS Business Entrepreneurship and Engineering
- 11 Facing the Future: Collaboration and Preparedness in Cybersecurity**
By Dave Christensen, CISSP, CCSA, NDRC, INFGP, INFG-InT, DevSecOps, Author, TACDA Member
- 14 Member Article: Retained-Heat Cooking**
By Tony M., TACDA Member
- 15 Cybersecurity is Everyone's Business: Protect Your Family**
By Bruce Curley, TACDA Vice President
- 19 Beginner's Long-Range Rifle**
By Jake C., TACDA Member
- 20 Two-Factor Authentication & Why You Need It**
By Bryson Meiling, MS Business Entrepreneurship and Engineering
- 23 Ready or Not Ready? Emergency Preparedness Quiz**
By US Navy
- 25 Cloud Security and Best Practices**
By Bryson Meiling, MS Business Entrepreneurship and Engineering
- 28 Personal Computer Safety**
By Martin Grady

WARNING:

When building a shelter, seek a professional design from appropriate, certified professionals, including electrical and civil engineers and ask to see the appropriate credentials from your builder and installer. Secure your area while under construction. Consult a geotechnical engineer to test your water table and soil type, and do not place your shelter in an area that could flood or accumulate water. Wet shelters could destroy and contaminate your supplies. You must keep entrances securely covered at all times. A poorly built or flooded shelter could result in death or injury from structure failure or dangerous levels of CO or CO₂ or other chemicals. TACDA and the authors of JCD journal entries offer this material as conceptual ideas, only, and cannot legally design your shelter nor can it ensure it has been safely constructed.

BOARD OF DIRECTORS

Jay Whimpey, P.E.
(*President*)

Bruce Curley
(*Vice President*)

Sharon Packer
(*Secretary*)

Gary Sandquist, Ph.D.
(*Treasurer*)

Bill Perkins
(*Board Member*)

ADVISORS

Paul Seyfried

Chuck Fenwick

Jane Orient, M.D.

Jonathan Jones, P.E.

Kylene Jones

Mary Pernicone, M.D.

Arthur Robinson, Ph.D.

John D. Hoyle Sr.

Christopher Fey

Colonel Jim Smith

Dr. Randall Smith

Christian Wilson

EXECUTIVE DIRECTOR

Roseanne Hassett

JOURNAL OF CIVIL DEFENSE

EDITORS

Brialyn Carlsen

Roseanne Hassett

Sharon Packer

GRAPHIC DESIGNER

Brialyn Carlsen

TACDA

PO BOX 1003

Sandy, UT 84091

www.tacda.org

info@tacda.org

Office: (800) 425-5397

Fax: (801) 662-0367

ISSN: 0740-5537

PRESIDENT'S MESSAGE



Cybersecurity is important for all of us. We receive a substantial amount of information and conduct much of our communications through the internet or other electronic means. Cybersecurity is not a complicated or particularly difficult endeavor, yet most individuals do not take even the most basic precautions.

In order to maintain appropriate cybersecurity on an individual basis, it is necessary to use strong passwords, not reuse passwords, use multifactor

authentication, keep software updated, and learn to recognize phishing scams. It is also wise to invest in anti-virus and malware software and use a VPN (virtual private network). These methods just take a little extra effort but are not particularly difficult. You can get help from the store where you purchased your computer or where you get your computer and/or phone serviced. You can also consult with the technical resources at your internet service provider, banking institution, and email service.

The government also has a website for CISA (Cybersecurity & Infrastructure Security Agency) that has a substantial amount of information about personal and organizational cybersecurity (<https://www.cisa.gov>). They provide free information and help to business, private, and government organizations.

I hope you will make the extra effort to navigate the cybersecurity journey and are able to keep your electronic resources operating efficiently.

Sincerely,

A handwritten signature in dark ink, appearing to read "Jay Whimpey".

Jay Whimpey, PE
TACDA President

FROM THE DIRECTOR

America's Next War

*By Roseanne Hassett,
Executive Director*

In October 2023, FEMA Administrator Deanne Criswell spoke to the National Emergency Management Association, highlighting the cybersecurity vulnerabilities facing our nation's critical infrastructure due to active threats from nation-states. She emphasized the importance of preparing for emerging threats like misinformation and cyberattacks, warning that "China will not just be hacking and stealing data in the future but is developing the ability to use the 'cyberverse' to aggressively disrupt and even destroy our critical infrastructure."

For instance, a cyber-attack on an electrical grid in a densely populated city could cause widespread panic and chaos like the Colonial Pipeline cyber-attack in 2021. This would most likely be even more devastating due to the serious issues caused by lack of electricity.

Administrator Criswell further stated that "our adversaries understand how to manipulate information to spread fear, anger, confusion, and distrust in the Government. In some cases, this is their clear goal. They understand how to use social media to create chaos. They have demonstrated a willingness to use cyber tools to hack and disrupt on a national scale. [They] won't be using vehicle-borne IEDs or flying aircrafts into buildings like the terrorist attacks on 9/11... our adversaries are far more likely to hijack our power grids, our telecom infrastructure, or our financial institutions, and disrupt our military's ability to mobilize."...

Continued on page 18.

SUBSCRIBE TO THE JOURNAL!

Electronics can often get damaged during natural disasters, and having the right information at your fingertips could be crucial to your survival.

When you subscribe to the Journal of Civil Defense, you will be mailed our publication twice per year in April and October.

\$15/yearly



The Importance of Cybersecurity for Protecting Infrastructure in America: Lessons from the Pipeline Attack

By TACDA Staff - AI Assisted



For this article, TACDA is trying something new. Artificial intelligence is part of our future. While that may be frightening, it can also be a very useful tool. To prove this, we asked ChatGPT this prompt. The article that follows was the response.

Prompt: Tell me about the importance of cybersecurity for America's critical infrastructure and what can be done to protect it. Include examples of a recent cyber attack that we can learn from.

In an increasingly digital world, the vulnerability of critical infrastructure to cyberattacks is a growing concern. For decades, American infrastructure systems such as energy grids, water supplies, and transportation networks have been largely dependent on a mix of legacy systems and modern digital technologies. While these advancements have brought efficiency and connectivity, they have also introduced new risks—specifically, the threat of cyberattacks targeting these vital systems. The Colonial Pipeline attack, which took place in May 2021, serves as a stark reminder of the dangers of cyber vulnerabilities and underscores the importance of bolstering cybersecurity measures to safeguard the nation's critical infrastructure.

THE COLONIAL PIPELINE ATTACK: A WAKE-UP CALL

The Colonial Pipeline cyberattack, one of the most high-profile incidents in recent memory, demonstrated just how devastating a cyberattack on critical infrastructure could be. Colonial Pipeline, which operates the largest fuel pipeline system in the United States, was forced to shut down its entire network after a ransomware attack crippled its operations. The company was targeted by the DarkSide ransomware group, which encrypted the com-

pany's data and demanded a ransom to restore access. The impact was immediate and widespread. The closure of the pipeline, which supplies fuel to much of the eastern United States, caused panic buying, fuel shortages, and skyrocketing gas prices. The disruption underscored how reliant the U.S. economy and daily life are on the smooth functioning of critical infrastructure systems. Beyond the immediate financial costs, the attack raised alarms about the potential for even more severe consequences if other critical sectors—such as water, electricity, or healthcare—were targeted.

While Colonial Pipeline was able to restore service relatively quickly, the incident illuminated vulnerabilities that could be exploited by malicious actors, whether they are state-sponsored hackers, criminal organizations, or even individuals with sufficient technical expertise. The breach also revealed how unprepared many infrastructure operators are when it comes to preventing and responding to cyber threats. If this attack had been part of a larger coordinated campaign, the consequences could have been far worse.

THE SCOPE OF CRITICAL INFRASTRUCTURE THREATS

Cybersecurity experts and government officials agree that critical infrastructure is one of the most attractive targets for cyberattacks. In the United States, critical infrastructure refers to systems and assets essential to the nation's security, economy, public health, and safety. This includes energy grids, water treatment plants, transportation systems, telecommunications, and financial services. A successful cyberattack on any of these sectors could lead to widespread disruptions, loss of life, economic chaos, and even national security crises.

For instance, consider the potential fallout of a cyberattack on the electrical grid. A malicious actor could exploit vulnerabilities in grid management systems to cause blackouts, damage electrical equipment, or even trigger cascading failures that affect large regions of the country. Similarly, a breach of water treatment facilities could compromise water supplies, making them unsafe to drink, potentially causing widespread illness or panic. The consequences of such attacks could be catastrophic, particularly if they occur simultaneously or as part of a coordinated effort by multiple threat actors.

Unfortunately, many of the systems that underpin these critical infrastructure sectors were built decades ago, at a time when cybersecurity concerns were not as pressing. As a result, these systems were not designed with modern cyber threats in mind. While many infrastructure operators have made efforts to upgrade their defenses, the pace of innovation in cybersecurity often lags behind the sophistication of cybercriminals. As a result, there is an urgent need for a comprehensive approach to cybersecurity in these critical sectors.

THE ROLE OF GOVERNMENT AND PRIVATE SECTOR COLLABORATION

Addressing the cybersecurity challenges facing critical infrastructure requires a collaborative effort between the government and the private sector. Many infrastructure systems in the U.S. are owned and operated by private companies, making it essential for these entities to take responsibility for their own cybersecurity. However, the government plays a key role in setting cybersecurity standards, providing guidance, and offering support in the event of an attack.

One of the most important steps that the government can take is to strengthen cybersecurity regulations and ensure that they are enforced. In the wake of the Colonial Pipeline attack, former President Joe Biden issued an executive order aimed at improving the nation's cyberse-

curity posture. The order included provisions to enhance information-sharing between the government and private sector, improve incident response capabilities, and require critical infrastructure operators to adopt stronger cybersecurity practices. However, regulatory action alone is not enough. Private companies must also prioritize cybersecurity as part of their overall risk management strategy.

The private sector must invest in the latest cybersecurity technologies and adopt best practices, such as regular patching and updating of systems, employee training to recognize phishing attempts, and the implementation of strong authentication protocols. Furthermore, companies must develop and test comprehensive incident response plans that can be quickly activated in the event of a breach. This includes creating redundant systems and backups to ensure that operations can continue if primary systems are compromised.

While government regulations and private sector initiatives are essential, cooperation between the two is key. The sharing of threat intelligence, for example, allows organizations to learn from each other's experiences and stay ahead of emerging threats. During the Colonial Pipeline attack, the FBI, the Department of Homeland Security, and the Cybersecurity and Infrastructure Security Agency (CISA) worked closely with the company to help mitigate the damage. However, greater collaboration is needed to create a unified and robust cybersecurity defense system for critical infrastructure.

STRENGTHENING CYBERSECURITY IN CRITICAL SECTORS

To improve cybersecurity in critical infrastructure, several key steps need to be taken across different sectors:

- 1. Adopt Zero-Trust Architectures:** Zero-trust security models, which assume that no entity—inside or outside the network—is trusted by default, can significantly enhance the security of critical infrastructure systems. By verifying every user and device before granting access to sensitive systems, organizations can prevent unauthorized access and reduce the risk of insider threats.
- 2. Implement Robust Backup and Recovery Systems:** Given the growing threat of ransomware, it is critical that infrastructure operators maintain secure and up-to-date backups of essential data and systems. Regularly testing these backups and having a recovery plan in place can ensure that organizations can quickly resume operations after an attack.
- 3. Enhanced Employee Training and Awareness:** Many cyberattacks, including ransomware attacks, begin with human error such as falling victim to phish-

ing emails. Training employees to recognize common cyber threats and encouraging a culture of cybersecurity awareness can go a long way in reducing the risk of successful attacks.

4. **Security by Design:** Critical infrastructure systems should be designed with cybersecurity in mind from the outset. This means integrating security measures into the architecture of new systems and retrofitting older systems with necessary updates. Additionally, cybersecurity audits should be conducted regularly to identify vulnerabilities.
5. **Public-Private Partnerships for Information Sharing:** Creating robust mechanisms for sharing information about cyber threats and vulnerabilities between the government and the private sector can help organizations stay informed about emerging threats and take proactive steps to defend against them.
6. **International Collaboration and Standards:** Cybersecurity is a global issue, and many of the threats facing U.S. critical infrastructure originate from international actors. Strengthening diplomatic ties and working with international partners to establish cybersecurity norms and standards is essential for combating global cyber threats.

CONCLUSION

The Colonial Pipeline attack was a wake-up call for the United States, highlighting the critical need to protect the nation's infrastructure from cyber threats. Cybersecurity is no longer just an IT issue—it is a national security issue that requires coordinated efforts across the public and private sectors. The lessons learned from the attack should drive meaningful changes in how we approach the protection of our critical infrastructure. By adopting a comprehensive cybersecurity strategy, improving collaboration between stakeholders, and investing in the latest technologies, we can better safeguard the nation's most vital systems against cyberattacks. The stakes are high, and the time to act is now.

Photo by Andras Vas on Unsplash



TACDA ACADEMY

A lesson manual created through the collaboration of civil defense experts, scholars, military personnel, and other professionals to teach the basics of survival in an easy-to-understand format.



Download **FREE**
or purchase
hard copy online
at tacda.org





RISKS

OF SMART HOME GADGETS

**By Bryson Meiling, MS Business
Entrepreneurship and Engineering**

Photo by Jakub Zerdzicki on Unsplash

Every night across America, families follow the same bedtime ritual: checking that doors are locked, security systems are armed, and windows are secured. Yet while we're busy fortifying our physical defenses, many of us are overlooking the digital doors we've installed throughout our homes. That smart thermostat controlling your heating, the security camera watching your front porch, and even the refrigerator ordering your groceries – each represents a potential vulnerability in your home's security.

The promise of convenience has led us to fill our homes with internet-connected devices that can control our lights, monitor our babies, and even feed our pets. But these seemingly helpful gadgets can also serve as silent gateways into our most private spaces. Unlike a broken window or a picked lock, digital breaches often go unnoticed until sensitive information has already been compromised or devices have been hijacked for malicious purposes.

The average American household now contains over twenty connected devices, creating an expansive digital perimeter that needs to be defended. But protecting your smart home doesn't mean giving up on the convenience of modern technology. Just as we've learned to secure our physical homes through practical habits and common-sense measures, we can strengthen our digital defenses through straightforward precautions and family protocols.

GROWING A SMART HOME BATTLEFIELD

The modern American home has become a web of interconnected devices, each promising to make our lives easier and more efficient. Walk into any household today

and you might find smart speakers awaiting voice commands, cameras monitoring every entrance, and even thermostats learning your family's schedule. These devices form an invisible network that touches every aspect of daily life – from how we secure our homes to how we put our children to bed.

But this convenience comes at a cost. Each connected device creates a potential access point into your home network. Unlike traditional burglars who leave physical evidence of break-ins, cyber intruders can silently collect data about your family's habits, movements, and conversations. They might monitor when you're away from home through your thermostat settings, access stored video feeds from your security cameras, or use your network-connected devices as stepping stones to reach more sensitive information like financial records or personal documents.

The threat isn't just from individual criminals. Smart home devices are increasingly targeted by sophisticated operations that can turn thousands of compromised devices into networks for larger attacks. Even more concerning, many of these devices store their data on servers outside our borders, where different privacy laws – or a lack thereof – determine how your family's information is protected and used.

UNDERSTANDING THE VULNERABILITIES

The weak points in your smart home's armor often stem from oversights that many of us make when setting up these devices. Think of each smart device as a small computer – it needs regular updates, proper configuration, and careful supervision.

The most common vulnerability: default passwords. Many families plug in their new devices and start using them immediately, never changing the factory-set passwords that can be easily found online by anyone with malicious intent.

Even when we do change passwords, our home networks often remain vulnerable. That basic WiFi router from your internet provider might be broadcasting your network's presence to the neighborhood with outdated security protocols. It's like having a sturdy front door but leaving all your windows unlocked. More concerning is how these devices talk to each other and share information. Your smart TV might be secure, but if it's on the same network as a poorly protected baby monitor, both become vulnerable.

Manufacturers themselves can introduce risks. Many smart home devices are designed to be "always listening" or "always watching," collecting data about your family's habits. This information isn't always stored safely – some companies keep it on poorly secured servers, while others might sell it to third parties. Even more troubling is the fact that many manufacturers stop providing security updates after a few years, leaving older devices increasingly vulnerable to newly discovered threats.

BUILDING YOUR DIGITAL DEFENSE

Securing your smart home doesn't require an engineering degree – it requires a methodical approach similar to how you'd secure your physical home. Start with your home's digital foundation: your WiFi network. Just as you wouldn't build a house on shifting sand, you shouldn't build your smart home on an unsecured network. Invest in a quality router that offers modern security features, and set it up with a strong password that combines random words, numbers, and symbols. Consider creating a separate guest network for visitors and another for your smart devices, keeping them isolated from the network you use for sensitive activities like online banking.

When adding new devices to your home, treat each one like a new door that needs proper locks. Take time to understand its security features before installation. Change default passwords immediately, enable two-factor authentication when available, and register your device with the manufacturer to receive critical security updates. Keep a detailed inventory of your devices, including model numbers and installation dates – this information becomes crucial when manufacturers release security patches or when devices reach the end of their supported life.

Your router's settings should be your first line of defense. Enable its firewall features, use WPA or WPA2

encryption if available, and regularly check which devices are connected to your network. If you spot something unfamiliar, treat it with the same suspicion you'd give to an unknown car parked in your driveway. For critical systems like security cameras or smart locks, consider devices that can operate locally without sending data to external servers, especially those based overseas.

Most importantly, establish family protocols. Create strong, unique passwords for each device and store them securely – a password manager can help with this task. Set regular times to check for and install device updates, just as you'd check your smoke detector batteries. Teach family members, especially children, about basic security practices like not sharing network passwords and being cautious about linking new apps to smart home devices.

EMERGENCY PREPAREDNESS AND BACKUP PLANS

Smart homes, for all their convenience, can become a liability during emergencies if we're not properly prepared. Power outages, internet disruptions, or system failures can render smart devices useless at critical moments. Every smart device in your home should have a manual backup plan – it's the digital equivalent of keeping flashlights and spare keys in strategic locations.

For critical systems like smart locks and garage doors, ensure everyone in your family knows how to operate them manually. Keep physical keys accessible but secure, and regularly test manual overrides to ensure they work when needed. Smart thermostats should be tested in their offline mode to ensure your heating and cooling systems remain functional without internet connectivity. For security cameras, consider maintaining a basic traditional camera system as backup, especially for critical entry points.

Document your home's digital infrastructure as thoroughly as you would your emergency supplies. Create

Continued on page 11.



Photo by Maria Ziegler on Unsplash

ARE YOU A MEDICAL EMERGENCY PROVIDER?

Save time and lives with

MEDICAL EMERGENCY TRIAGE TAGS

In a mass casualty incident (MCI), many more lives can be saved with the use of a medical emergency triage tag. METTAG triage tags are precise, fast, easy-to-use, and are utilized throughout the world.

METTAG FEATURES

- Enables first responders to promptly and accurately assess victims of an MCI
- Made from high-density, damage-resistant, synthetic material for use in harsh environments
- Resists fire, water, sunlight, chemical irritants, chemical disinfectants, and tearing
- Equipped with a 30" elastic cotton string to attach to a victim's body
- Unique sequential bar coding to identify the victim and their belongings



WHEN LIVES COUNT, COUNT ON METTAG! [HTTPS://WWW.METTAG.COM/](https://www.mettag.com/)
Visit our website for pricing or become a distributor. Call or email for details.

WWW.METTAG.COM

MT-501

- Patterned after the S.A.L.T. triage algorithm; Sort, Assess, Life-saving interventions, and Treatment/Transport
- Encouraged use by the NHTSA
- Incorporates a fifth tear off label for "Expectant"
- Sequential numbering system with barcode



MT-137

- Universal tool, with no language barriers, and minimal training for use
- Standard graphic symbols and a four-color tear-off triaging system
- Sequential numbering system with barcode
- Simple and effective tag for fast triaging in the field

MT-FLEET TAG

- For tracking fleet vehicles and maintenance needs
- Five-color tear-off organization system
- Quick and accurate recording of vehicle status
- Sequential numbering system

Call or email for sample
info@mettag.com

1-800-425-5397



Train your team using stock paper tags, without disposing of the more expensive synthetic tags. Training tags can now be purchased pre-tied. All tags measure 8 1/4" and 4."

a secure, offline record of all device passwords, model numbers, and account information. Store this information alongside your other emergency documents, and ensure trusted family members know how to access it if needed. Just as you maintain emergency food and water supplies, consider keeping basic non-smart replacements for critical devices – a simple programmable thermostat or traditional baby monitor could prove invaluable during extended outages.

CONCLUSION

Your home's digital security is just as crucial as its physical locks and barriers. While we can't control every threat in our increasingly connected world, we can choose how we prepare and protect our families. Every smart device you add to your home is both a convenience and a responsibility – a digital key that must be safeguarded with the same vigilance as the physical keys in your pocket.

Start today: check your router's settings, update your devices' passwords, and gather your family to create an action plan. Remember, a truly smart home isn't just about convenience – it's about maintaining control over your family's privacy and security in an interconnected world. The digital fortress you build today will help ensure your family's safety tomorrow.

Bryson Meiling is a software engineer, consultant, and writer with experiences in healthcare, manufacturing, and cloud technologies. He received a masters of science in business entrepreneurship and engineering from the University of Notre Dame. He enjoys working out, climbing, skiing, hiking, and Notre Dame Football. Most of his and his wife's time is taken up by their young, twin daughters who run around with big, toothy grins. He has a blog on Medium where he has his takes on technology and programming.



FACING THE FUTURE: COLLABORATION AND PREPAREDNESS IN CYBERSECURITY

By Dave Christensen, CISSP, CCSA, NDRC, INFGP, INFG-InT, DevSecOps, Author, TACDA Member

Years ago, discussions about security often focused on protecting our land, homes, and the right to defend ourselves. But what does that mean in today's world? Are we able to protect ourselves? Have the threats to our homeland evolved? This [article](#) by FEMA makes it clear that these threats have shifted and escalated to frightening levels.

In the article, FEMA Administrator Deanne Criswell discusses the increasing complexity of disaster response due to climate change, cybersecurity threats, and nation-state adversaries. She gives examples of what a nation-state attack might look like and offers solutions to



combat this type of crisis. Criswell emphasizes the importance of preparing for emerging threats like misinformation, cyberattacks, and attacks on critical infrastructure, advocating for stronger information-sharing, partnerships, and proactive planning to address these challenges.

Are we aware of the risks that cyberattacks could pose to our way of life? To our economy? To our loved ones? No one wants to write about risks without providing a silver lining, so take this as a wake-up call to act. Local governments tell the public that they are doing all they can to protect critical infrastructure; however, it is not that simple. Most critical infrastructure is managed by the private sector, but effective protection requires collabora-

Photo by Adi Goldstein on Unsplash



tion with the Cybersecurity and Infrastructure Security Agency (CISA).

PARTNERSHIPS

In 2018, the Department of Homeland Security (DHS) established CISA through the CISA Act, providing tools, resources, and guidelines to government agencies, businesses, and the public sector to enhance security and resilience in protecting critical infrastructure from cyberattacks. There is no magic solution to address the risks highlighted in the FEMA article, but we can implement layers of support to mitigate these risks while preserving the integrity of our ecosystem.

What can be done? Start at home. Learn how to use your phone and computer safely; understand how to do your job securely. Cybersecurity involves using strong, unique passwords for each account. While it can be challenging, the effort is worth it for your safety. Avoid clicking on suspicious links or text messages. Taking a moment to investigate before clicking can go a long way in preventing cyber-attacks.

Report suspicious activity or volunteer to help address larger risks within your workplace or local municipality. While it is easy to wait for others to solve problems, we must take the initiative and do what we can to promote a secure cyber environment.

To help private sectors combat cyber threats, CISA has developed a program called Shield's Ready, which is about taking action before an incident occurs so resilience becomes a reality.

"Shields Ready drives action at the intersection of critical infrastructure resilience and national preparedness...By taking steps in advance of an incident, organizations, individuals, and communities are better positioned to quickly adjust their posture for heightened risk conditions, in turn helping to prevent incidents, to reduce impact, and get things back to normal—as quickly as possible. Being part of the resilience journey makes for more resilient people, organizations, and communities."

CISA LISTS KEY STEPS TO BUILDING RESILIENCE

1. Identify Critical Assets and Map Dependencies:

Determine the systems that are critical for ongoing business operations and map out their key dependencies on technology, vendors, and supply chains.

2. Assess Risks:

Consider the full range of threats that could disrupt these critical systems and the specific impacts such threats could pose to the continuity of operations.

3. Plan and Exercise:

Develop incident response and recovery plans to reduce the impact of these threats to critical systems and conduct regular exercises under realistic conditions to ensure the ability to rapidly restore operations with minimal downtime.

4. Adapt and Improve:

Periodically evaluate and update response and recovery plans based on the results of exercises on real-world incidents and an ongoing assessment of the threat environment.

By implementing these practices, critical infrastructure entities and private sector organizations can be more resilient and return to normal business operations more quickly after an attack. After an exploit occurs, attention shifts to those who are prepared – whether it's local collectives like non-profits, the Red Cross, churches, or individual citizens. Following that, the focus turns to the actions of local and federal governments. Each of these groups plays an essential role in the recovery process.

US INTELLIGENCE REPORTS SUMMARIES

2022

The FEMA article directs readers to reports from the Office of the Director of National Intelligence (ODNI), which provide valuable insights into global security challenges.¹ The 2022 U.S. intelligence report paints a complex global security picture. It highlights intense competition and conflict between major powers, along with ongoing threats from groups and countries around the world.

- China is a primary rival to the U.S., expanding its military might and technological capabilities.²
- Russia remains a formidable challenge. It is using military, security, and intelligence tools to advance its interests, especially in its immediate region.
- Iran is a regional threat and continues to pursue nuclear ambitions and support proxy groups to counter U.S. influence. Its ballistic missile program and ties to terrorist organizations are concerning.
- North Korea's nuclear and missile programs, as well as its cyber activities, are still a major security risk.
- The 2022 report conveys a tone of deep concern, emphasizing the evolving threat landscape and the difficulties in responding effectively.

2024

The 2024 U.S. intelligence report identifies a fragile global order characterized by intensifying power competition and unpredictable transnational challenges.³

- China remains a major competitor seeking regional dominance and global influence. While facing economic challenges, its assertive actions regarding Tai-

wan, its technological advancements, and its military modernization pose significant threats.

- The war in Ukraine continues to be a defining factor, significantly impacting Russia's relations with the West. Domestic instability within Russia remains a possibility. Meanwhile, Russia continues to develop its nuclear and missile capabilities, deepening its ties with China.
- Cybercrime remains a significant funding source for various malicious actors. Digital authoritarianism and transnational repression are also growing concerns, exacerbating existing vulnerabilities, driving migration, instability, and conflict.
- The Gaza conflict exemplifies how such crises can create global ripple effects.
- Food insecurity is a major concern.
- ISIS and al-Qaeda affiliates, particularly in Africa, remain active threats.

Potential conflicts between India and China, India and Pakistan, and Azerbaijan and Armenia are highlighted, along with internal conflicts in regions such as the Balkans, Afghanistan, Sudan, Ethiopia, the Sahel, and Haiti.

OUR RESPONSE

Risks to our nation include natural as well as man-made disasters, and we must prepare for them all as best we can. While no one wants to hear that we need to plan for cyber-attacks or power outages, more and more people are taking proactive steps and installing local generators. It seems the public is becoming increasingly aware of these risks and more willing to do their part to mitigate them. However, there is still a long way to go.

Power outages are a common risk that can be diminished with proper planning. Keep flashlights and candles readily available, and plan for food preservation by ensuring refrigerators and freezers remain closed during an outage. Make sure needed medications are in good supply. Partner with neighbors to share resources or collaborate on obtaining missing food items during emergencies.^{4,5} Being creative with alternate energy is also a great choice (for example, adding a wood stove for use in winter).⁶

Don't panic, think through needs in advance, modify your lifestyle to help address risks, and plan accordingly. One easy step for me was to purchase storable meals to keep long-term in addition to our existing pantry of perishable and canned foods.

If local emergency services are not available, what can we do? I used to live on a mountain where we received three to four feet of snow each year. We were often snowed in, so we learned to manage many things on our

own, including dressing serious wounds, treating fevers, and managing other emergencies. Having some training and adequate supplies can be immensely helpful in situations where medical care is hours away or unavailable.

Finally, share ideas with friends and members of your community who are already considering how to address the risks posed by cyberattacks and their potential impact. I am not suggesting we implement everything listed, but even adopting some of the ideas, such as having a go-bag and preparing for blackouts, can better equip us for emergencies. I visited a local farm this year that belongs to a cooperative group that shares resources in the event of certain crises. I was impressed by their thoughtful planning and welcomed the opportunity to see people working together to address serious risks.

We need to return to that mindset of mutual support and preparation, particularly when it comes to cybersecurity and resilience in the face of technological threats.

I believe the solution lies in active involvement. Engage in each other's lives, support one another's well-being, and stay informed about the risks to our way of life – including cyber threats – and the steps being taken to address them. The alternative — isolation, finger-pointing, and waiting for others to solve our problems — only hinders progress.

References:

1. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community>
2. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/3597-2022-annual-threat-assessment-of-the-u-s-intelligence-community?highlight=WjwIlo=>
3. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>
4. <https://www.ready.gov/power-outages#:~:text=Preparing%20for%20a%20Power%20Outage&text=Plan%20for%20batteries%20and%20other,long%20battery%20backup%20will%20last>
5. <https://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies/power-outage.html?srltid=AfmBOopojx-ZtZGkDcLdYGFw-fReiRHKpfYIoXq6urPnqQjhBHf3KQEaI>
6. <https://forgenflame.com/blogs/forged-and-flame/alternative-heat-sources>

Dave Christensen is a principal systems architect focusing on security and architecture for a Fortune 500 company and the current chapter president for InfraGard NJ.

MEMBER ARTICLE

RETAINED-HEAT COOKING

By Tony M., TACDA Member

We have all heard cliché sayings around preparedness, with often too little strategy, practicality, or follow through to the advice. While this article focuses on the first pillar of the saying, there is much left to be desired from the other two in the community. Storing dried beans and rice for long-term storage is easy, cheap, and a great recommendation for those getting started with the idea of food storage.

Like many, I bought my dried beans and rice, stored it away, and felt good about it. I later came to an important realization: if I don't have access to electricity, and fuel is in short supply, how am I going to cook dried rice and beans that normally take hours to simmer on a hot stove? Enter retained-heat cooking. The concept is simple and has been around for generations. Bring your food up to cooking temperature then remove from heat and put it in a highly insulated container to continue the cooking process. The intent of this article is to make this process easy, reproducible, and scalable. One food jar can easily make a meal or a solid base for a meal for one person. It can be cooked in five minutes and tossed in a backpack or car to complete the cooking process and be eaten later. All of the items used are from a very common retail store, found in the camping section. You will need a 22-ounce vacuum insulated food jar, small propane stove, 1-lb propane bottle, cooking pot, dried white rice, and water.

DRIED WHITE RICE INSTRUCTIONS:

1. Place 2 cups water and 1 cup rice in pot. Bring to a boil then turn heat to low with the lid on.
2. Boil for five minutes, put rice and water in food jar, seal tightly for one hour. Done!

At initial testing, the rice was still at 180 degrees F when I opened the food jar after an hour. This produces about 2.5 cups of rice when complete. Two and a half cups of white rice is 40% of your daily requirement for carbohydrates, and just over 500 calories. Camping tip: combine this with a can of soup and you have an easy and portable meal for two people! Add butter and salt to taste.

At an elevation of 1,000 feet above sea level on a moderate spring day (50 degrees Fahrenheit), it took three minutes to cook the rice on low heat. One-pound pro-

pane tanks can run a single-burner camp stove for around three hours on high. You should be able to cook eight jars of food on a single bottle of propane. A single bottle of propane could be enough fuel for a week of warm lunches for one person.

DRIED PINTO BEANS INSTRUCTIONS:

1. Soak one cup of beans with three cups of water overnight.
2. Add three more cups of water, boil for 15 minutes with the lid off.
3. Place in larger vacuum insulated food jar, let sit for four hours. Done!



Tony is a proud husband and father of three. He is a volunteer firefighter, EMT, amateur radio operator, and outdoor enthusiast.

HAVE A SPECIAL SKILL? WANT TO SHARE YOUR PREPAREDNESS KNOWLEDGE?

Tacda members, submit an article to be considered for publication in our next journal! Email articles (subject: member article) to info@tacda.org.

CYBERSECURITY IS EVERYONE'S BUSINESS: PROTECT YOUR FAMILY

By Bruce Curley,
TACDA Vice President

Photo by Artem Bryzgalov on Unsplash

Like civil defense, cybersecurity is everyone's business and is especially critical for families. Protection from cyberattacks is no longer just the business of the government or experts. It is a fundamental responsibility of every American family.

You must know how to defend against social engineering ruses, phishing attacks in all their variations, cell phone calls from cybercriminals, and other cyber threats. More importantly, you must train your children and grandchildren in the tools they need to deflect and defeat these real-world threats to their freedom. Small businesses and average Americans are being fleeced out of money by cybercriminals.

Some of these cybercriminals operate on their own. Some are employed by their governments. The Communist Chinese Party's (CCP) 50 Cent Army (cyber warriors) has tens of thousands of hackers who act as nefarious bots. This [video](#) provides additional information on the 50 Cent Army.

Some cybercriminals act on their own (and with their government's approval) to steal money, intellectual property, home titles, reputations, and other goods and services from Americans.



Here, I will analyze what you can do when cybercriminals and hackers strike.

PREDATOR CYBERCRIMINALS PREY ON AMERICANS DAILY

Every day, Americans lose millions of dollars from predator cybercriminals, mostly foreigners. What you

read in the media is just the tip of the iceberg. The issue is much bigger since most companies and individual Americans are so ashamed to have fallen for a grift that they do not report it to law enforcement.

Even if they do report it, local law enforcement does not have the resources to investigate it. National law enforcement knows that most cybercriminals are overseas. The reality is that 99.9% of cybercriminals will never be caught or prosecuted.

You are on your own. So you need to learn to identify cybercriminals when they attempt to manipulate you to gain access to your credit card, money, bank account, or data.

U.S. GOVERNMENT REPORTS OF CCP CYBERSECURITY ATTACKS

The U.S. National Institute for Standards and Technology (NIST) released the new version of its Cybersecurity Framework (CSF) on Feb. 26, 2024. The CSF is designed to support the implementation of the 2023 National Cybersecurity Strategy. It defined the Communist Chinese Party (CCP) as "the broadest, most active, and most persistent threat to both government and private sector networks."

The publication of the new CSF followed the publication of a guidance document by the Cybersecurity and Infrastructure Security Agency (CISA) warning that China's attempts to infiltrate, disrupt, and destroy vital U.S. facilities could endanger American lives. "Chinese state-sponsored cyber actors are seeking to pre-position

themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure for a major crisis or conflict with the United States,” the advisory said.

The malware, it said, was devised “to launch destructive cyber-attacks that would jeopardize the physical safety of Americans and impede military readiness.” That warning followed Congressional testimony by senior intelligence leaders that revealed the U.S. intelligence community had eradicated a Chinese botnet from more than 600 routers associated with critical U.S. infrastructure. That infrastructure included water, gas, energy, rail, air, and port traffic control systems.

Rep. Mike Gallagher (R-Wis.) described the malware as “the cyberspace equivalent of placing bombs on American bridges, water treatment facilities, and power plants. There is no economic benefit for these actions. There is no intelligence-gathering rationale.

“The sole purpose is to be ready to destroy American infrastructure, which will inevitably result in mass American casualties.” These daily CCP cybersecurity attacks may seem far away, but they can lead to serious manmade disasters for you and your family, so you need to be aware of them.

These are cybersecurity threats against American infrastructure that support your family’s standard of living and well-being. They are a potential apocalyptic disaster that continuously happens in cyberspace. Your taxes support government experts (who also employ private sector experts) who hopefully do their job and prevent these cyberattacks on our infrastructure from becoming an existential threat.

There is another level to this cybersecurity attack being waged daily against your family. It constantly probes into your computer and cell phone in hopes of exploiting vulnerabilities whereby they can scam you out of your life savings. Below are just two examples.

HOW TO PROTECT YOUR DATA AND MONEY FROM CYBER-CRIMINAL COMPUTER ATTACKS

Your email and texts are windows of opportunity for cybercriminals. There are a variety of these kinds of scams, but here is one example:

Someone on X contacts you claiming to be a relative of “Elon Musk” who tells you they appreciate your support for him. Then more and more relatives of “Elon Musk” contact you on X with effusive praise and state that “Elon” wants to thank you and provide you with his contact information, a Telegram account where you can chat with him. They are clear that you should not share this information with anyone.

You go to the Telegram account and the fake “Elon

Musk” is also effusive in his praise of your fan support. He wants to reward you by giving you access to his Bitcoin investment platform – a perk for a few fans. He provides a link where you can set up an account and then instructs you on how to buy Bitcoin and transfer it to his Bitcoin investment platform.



You set up the account and transfer money into it. And what do you know, your investment triples in worth the first day. Against your better judgment, they exploit the principle of imaginary low risk and high reward that makes state lotteries and casinos so profitable, the endorphins kick in, and you transfer more of your hard-earned money into your new “investment” account hoping to get something for nothing.

You invest \$1,800. You receive daily email updates from cybercriminals that show rapid growth of your initial investment. They tell you not to disclose details to anyone in fear of being caught by the authorities.

The problem is: it’s all a sophisticated scam. Once the cyber thieves decide they have enough of your money, the account disappears overseas, you have lost your savings, and they move onto the next victim. This – or countless variations of this scam – happens every day.

You can report the cybertheft to the company from whom you purchased the Bitcoin, to local law enforcement, or even the FBI ([ic3.gov](https://www.ic3.gov)), but you will not see your money again.

Often times, it does not end there. Shortly after this scam, the “real Elon Musk” contacts you via X and provides another Telegram account to call him. If you do, he informs you that the people who just stole your money cloned his investment platform, “Tesla Cybrox Pro.” He regrets that, wants you to invest in his actual investment platform, and for \$500, promises he can locate the cybercriminals who fleeced you out of your savings.

Again, this is just one example of many sophisticated cyber scams that are going around to steal American money.

HOW TO PROTECT YOUR DATA AND MONEY FROM CYBERCRIMINAL CELL PHONE CALLS

There are many variations on this attack, but it goes something like this. Out of the blue, you get a call. It is not from family or friends or anyone you know. On the other end, someone identifies themselves as a representative from Microsoft and says your computer has been hacked, and they need to take over your system to help protect your data. They will bait with something clever like, "I am calling from your bank because there has been unusual activity on your account."

You could get a call from your bank that a cybercriminal is draining your bank account, and he patches you through to an "FBI agent" who confirms it. Then they inform you that you need to go to your bank, withdraw the remaining funds, and transfer them via Bitcoin back to your bank through an account number they will provide to avoid the "cybercriminals" who have hacked your account to preserve your remaining funds.

You may get a call from a cybercriminal claiming they are the police, and that your grandchild needs \$1,000 bail or they will spend the night in jail.

When you get these calls, hang up. They are trained. They are skilled. They are clever. They are devious. They will manipulate you.

Do not allow them to have access to you or your thoughts. Practice "Zero Trust". Only answer your cell phone if you know the number or the person calling. If you do not recognize the number, do not answer. If the person calling is legitimate, they will leave a message. Dishonest cybercriminals, for the most part, will not leave a message. They will simply move on to the next victim.

CHECK YOUR BANK ACCOUNTS FOR UNUSUAL ACTIVITY

The most common cybercriminal scam involves gaining access to your credit card or checking account and running a \$9.99 or some other small amount to see if it clears. If it does, they return and clean out your account.

I had this happen three months in a row with three different debit cards. The cybercriminal would try to put through small \$9.99 charges on my debit card. They were for gaming sites, and I do not game, so I contacted my bank and got a new card. The cybercriminal was able to access the next two cards as well.

How?



Photo by Avery Evans on Unsplash

Neither I nor my bank could find out. This is a common scam and one you can prevent by closely monitoring your checking, savings, debit and credit accounts for unusual charges or activity. Your bank can identify certain unusual activities, but not all.

You are on your own when it comes to these cybersecurity scams, and you must prepare yourself and your family.

BEWARE OF CYBERSECURITY SCAM TAG TEAMS

Some cybercriminals practice a very sophisticated tag team methodology. Here is one of many schemes they use:

One foreign cybercriminal calls and states that you have been identified as spending money on child pornography by the FBI due to charges on your bank account. When you laugh at them and say that is impossible, they will ask you to hold, and they will claim a representative of your bank is on the other line and they will patch you through to them.

Another perp will come on the line and state he is a representative from your bank and that there are, indeed, payments on your account paying for child porn. He will identify your bank and explain that he needs to take control of your computer and review your account for unusual activity. Then another perp will come on and announce that he wants to work with you to keep the remaining amount in your account safe. The criminal will ask you to withdraw it to protect it and go to a crypto ATM to transfer it back to the bank.

There are many variations on this scenario, but it is a technique they use to convince honest Americans to empty their bank account. Hang up before they get to the tag team.

BACK UP YOUR FAMILY DATA

It is vital that you back up your critical family data. The reason small businesses do not survive after a disaster is no longer the event itself but the loss of data. Because small businesses lose their business records, they cannot get up and running after a disaster.

The same holds true for a family's data. Be sure to back up your family data. An easy way to do so is to order one or more EMP-resistant, waterproof, USB drives from the [TACDA Survival Store](#). As a bonus, these thumb drives come pre-loaded with the TACDA emergency resource essentials.

BE READY

You must be aware of cybercriminal threats and attacks. They are endless. Once a cybercriminal steals your data or money, they will not be identified or prosecuted as they are safe overseas. So learn what you need to do to protect yourself.

There are many resources to help you. Consider reading this [article](#) by the Washington Post about a woman scammed into believing she was an FBI 'asset', consequently losing her life's savings. Scott Augenbaum is a cybersecurity expert who provides training on staying safe in our digital world. Check out his website [here](#).



Washington Post
Article

Scott Augenbaum

Bruce Curley is the volunteer Vice President of TACDA. He has done professional and volunteer civil defense work for over 40 years. You can find 25 years of his civil defense strategies on <https://poetslife.blogspot.com/> and more recently on Substack at <https://poetslife.substack.com/>.



Photo by Towfiqu Barbhuiya on Unsplash

FROM THE DIRECTOR

Continued from page 3

These threats are not just a possibility but a looming reality, and many attacks have already occurred. Fortunately, there are steps we can take to impede future cyber-attacks. Through the Shields Ready campaign found on CISA.gov, (<https://www.cisa.gov/shields-ready>.) FEMA has created plans to help municipalities mitigate risks by "making resilience during incidents a reality by taking action before incidents occur."

We encourage you to actively participate in this initiative and share your success and knowledge with others. Together we can make America stronger and face the realities of the future with confidence and success.



DONATE

TACDA would not exist without the generous donations and support of its members. Because of you, TACDA can continue its mission to educate and empower Americans to survive any disaster or emergency.

All donations given to The American Civil Defense Association are tax deductible. Save your receipts!





BEGINNER'S LONG-RANGE RIFLE

By Jake C.,
TACDA Member

CREDENTIALS

I am simply a hobbyist, enthusiast, and civilian with opinions. I spend time learning about gear and skills and doing my best to accumulate both high quality tools and accompanying techniques to improve at the art of shooting. I don't purport to be anything more than that. My opinions have been formed over years of dwelling in online forums and verifying with my own purchases. I have a small collection, as I am a young father who avoids funding any hobby with debt. So, read along if you like, and perhaps, I can expose you to some great products made by high-quality manufacturers. There's so much good out there!

PHILOSOPHY

I am a believer in "buy once, cry once" or quality over quantity. Everyone knows someone who loves gear and collects several pieces of questionable reputation – probably too many to even use with any regularity. People love to collect, I get it. I do my best to reign in my materialistic side by saving until I can buy the best I can reasonably afford. It takes more time to acquire the nice stuff, but it comes with a sense of satisfaction and confidence that your tools will function when you need them most.

MY RECENT PROJECT

I recently entered the world of long-range rifles. When you start shooting long range, people have two primary considerations, among many others: a lightweight rifle, suitable for carrying and hunting in the mountains or an accuracy-focused rifle, which typically comes with a little more weight.

Having little background in either hunting or long-range shooting, I wanted a rifle that would enable me to learn on my own, which means I need to be able to track

my own misses. This is easiest with a slightly heavier rifle and a short action cartridge. After lots of research, I acquired a Seekins Precision Havak HIT in 6.5mm creedmoor.

Seekins is a great company building high-quality rifles and components in Idaho. If you haven't seen their products, I would encourage you to check them out. As a testament to the quality of the rifle, I had a first round impact on steel at 575 yards in my second session with the rifle.

It's been very exciting to start something new and realize small victories from learning and practice. There is a lot of great information on the internet. I've particularly enjoyed watching content from shooters like Phil Velayo and Joe Dawson. While I'm still a novice, I'm enjoying the journey and looking forward to continuing to develop the skill.

BUILD LIST

Rifle: Seekins Havak HIT 6.5mm creedmoor

Scope: Leupold MK4 HD 6-24x52 PR2 (Figures 1 and 2)

Rings: RRS-SOAR Uniblock 34mm (Figure 1)

Bipod: Atlas CAL BT65-NC (Figures 3 and 4)

Bipod Clamp: RRS-SOAR SC-ARC (Figures 3 and 4)

Arca Rail: RRS-SOAR USR-340mm (M-Lok)

Muzzle Device: Area 419 Hellfire Match (Figure 5)

Anti-Cant Device: Flatline Ops Sniper-X (Figure 6)



Figure 1



Figure 2



Figure 3



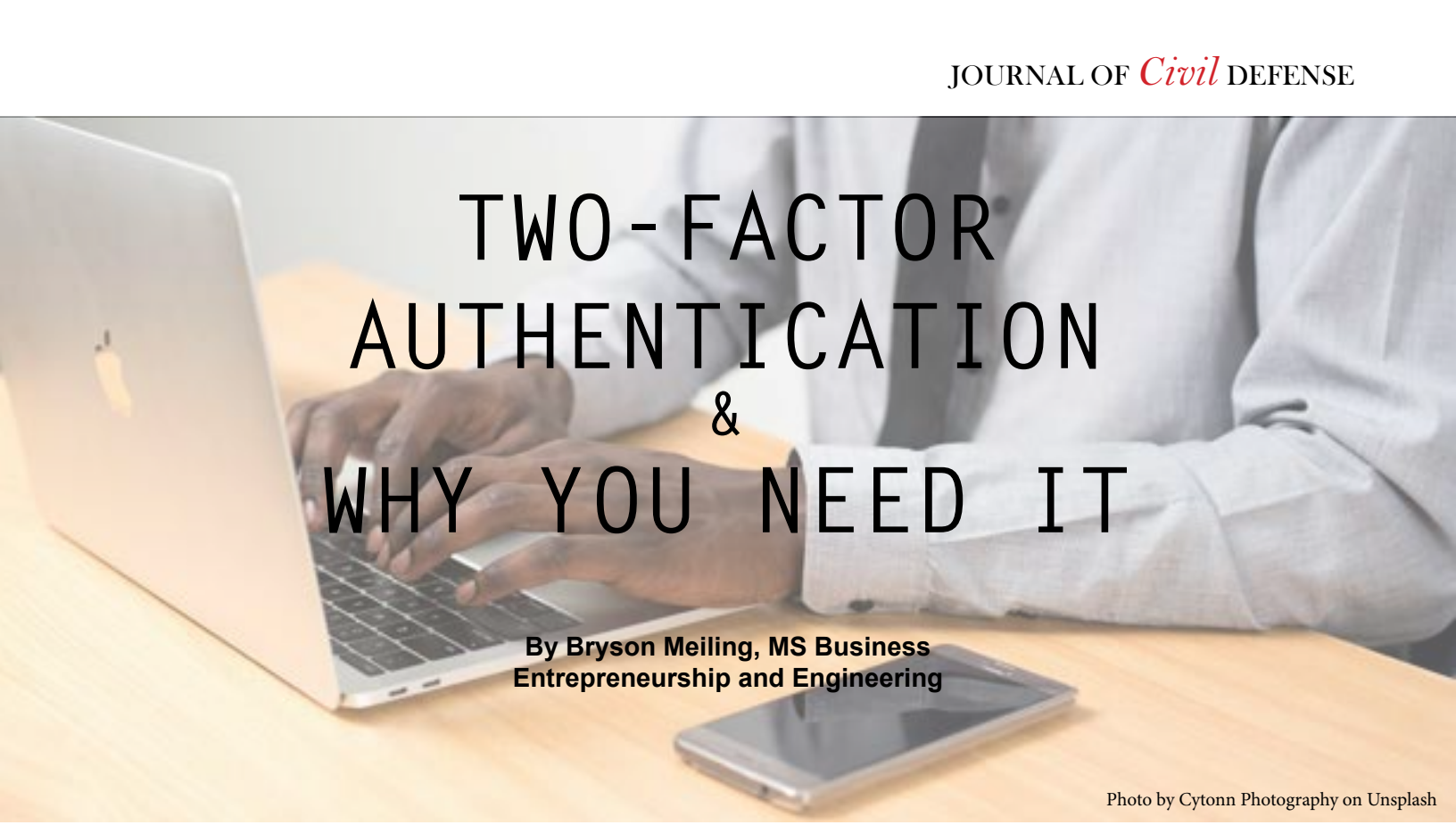
Figure 4



Figure 5



Figure 6



TWO-FACTOR AUTHENTICATION & WHY YOU NEED IT

By Bryson Meiling, MS Business
Entrepreneurship and Engineering

Photo by Cytonn Photography on Unsplash

Imagine waking up on a crisp morning. You fix breakfast, grab your travel mug, and head out the door, carefully turning the deadbolt to secure your home. But just steps from your front porch, a thought stops you cold: did you check that living room window? The one right next to the door? In our rush to follow basic security habits, we sometimes miss the obvious vulnerabilities hiding in plain sight.

Cybersecurity works the same way. We create complex passwords, thinking we've locked our digital front door, while leaving other entry points wide open. Hackers, like opportunistic thieves, don't always try to break through your strongest defenses – they look for the easiest way in.

This is where two-factor authentication (2FA) comes in. Think of it as not just locking your front door but installing a comprehensive home security system. It's about securing every possible entry point to your digital life. Instead of relying on a single lock (your password), 2FA adds multiple layers of security, like having both a deadbolt and a security system protecting your home. Just as you wouldn't protect your family with just a basic door lock these days, it's time to move beyond simple passwords for our digital security.

THE PASSWORD PROBLEM

The most common and simple form of authentication today is using an email and a password. If you ever lose

your password, the website will send an email asking for you to reset your password. While on the surface this seems secure, let's talk about the "open window" that might allow someone to access your account. Perhaps the hacker can access your email or guess your password. This form of authentication is simply not enough for your valuable data and privacy. There are multiple ways around it, and frankly, most people don't use adequate passwords.

Seventy percent of passwords can be guessed in a fraction of a second! This means that the password you've had for years, while adding an exclamation point occasionally, is simply not secure if you ever find yourself in an unfortunate situation. If you are part of the group that recycles passwords, you are part of a reported 30% who do this. Only 20% of people use unique passwords for every account.

UNDERSTANDING TWO-FACTOR AUTHENTICATION

Think about picking up your child from school. The school doesn't let just anyone walk in and take a student home. First, you have to show your ID (something you have), and then the staff checks their approved pickup list (something they know about you). This double-check system keeps our children safe from unauthorized pickups. Two-factor authentication works the same way for our digital lives.

In the digital world, two-factor authentication (2FA)

adds a crucial second layer of security beyond just your password. Just like how the school uses two different ways to verify parents, 2FA requires two different types of proof that you are who you say you are. Security experts break these proofs into three main categories:

Something you know: This is typically your password, like “Open Sesame” with Ali Baba and the Forty Thieves. But unlike the fictional cave of treasures, a password alone isn’t enough anymore to protect your digital valuables.

Something you have: This could be your phone, where you receive a text message code, or a special security key you carry on your keychain. Think of it as your digital house key – except this key changes every time you use it and/or can’t be copied by thieves.

Something you are: This refers to biometric data like your fingerprint or face scan. While not commonly used for website 2FA, you might already use this when unlocking your phone or laptop.

When you enable 2FA on your accounts, you’re essentially installing a double-lock system for your digital life. Even if someone manages to guess or steal your password, they still can’t break into your account without that second factor. It’s like a thief having your house key but being stopped by the security system – they simply can’t get in without both.

This extra step might seem inconvenient at first, like having to sign in at the school office instead of just waving through the window. But just as we gladly accept school security measures to protect our children, this small extra effort in our digital lives can prevent devastating account breaches and protect our families’ financial and personal information.

COMMON 2FA METHODS: CHOOSING THE RIGHT PROTECTION FOR YOUR FAMILY

Just as we have choices in how to secure our homes – from basic deadbolts to advanced alarm systems – there are several ways to add two-factor authentication to your accounts. Let’s examine the most common methods, starting with the simplest and moving to the most secure.

TEXT MESSAGE CODES

The most widely used form of 2FA is the humble text message code. When you try to log in, the service sends a short code to your phone. It’s popular because almost everyone has a cell phone, and it’s easy to understand. Many banks and social media sites default to this method.

However, text message 2FA has some concerning weaknesses. Imagine if a criminal could convince the post office to forward all your mail to a different address – that’s similar to what happens in a “SIM swapping” attack. Criminals can sometimes trick phone carriers into transferring your phone number to their device, letting them receive your verification codes.

Additionally, text messages can be delayed or fail to arrive when cell service is poor, leaving you locked out of your accounts when you need them most.

AUTHENTICATION APPS

A more secure option is using an authentication app like Google Authenticator or Authy. These apps generate time-based codes that change every 30 seconds. Think of it like a special padlock that constantly changes its combination, but only you and the service you’re logging into know the pattern.

These apps work even without cell service or internet connection, making them more reliable than text messages. They’re also immune to SIM swapping attacks because they’re tied to your specific phone, not your phone number. The main drawback? If you lose your phone or get a new one, you might need to go through some extra steps to regain access to your accounts. Some apps can back up this private data to the cloud. Password manager apps like Password1 or Enpass can also handle these rotating codes.

PHYSICAL SECURITY KEYS

A high standard in 2FA is the physical security key – small devices that look like USB drives or keychains. Companies like Yubikey make these, and they’re virtually unbreakable by hackers. It’s like having a high-security key that can’t be copied at the hardware store.

When you log in, you simply plug in or tap the key to your device. There are no codes to type, nothing to intercept, and no way for someone halfway around the world to trick the system. Major tech companies require their employees to use these keys because they’re so secure. The downside? They cost money (usually \$25-50), and you’ll want backups in case you lose one. But for protecting your most valuable accounts, especially financial ones, they’re worth considering as part of your family’s digital emergency preparedness kit.

CHOOSING YOUR METHOD

For most families, using an authentication app provides the best balance of security and convenience. Save the physical security keys for your most critical accounts,

like your primary email and financial services. Text message codes, while better than no 2FA at all, should be viewed as a temporary solution while you transition to more secure methods.

Remember, just as you might have different locks on your front door versus your garden shed, it's okay to use different levels of security for different accounts. The important thing is making the choice to add that extra layer of protection to keep your family's digital life secure.

PRACTICAL IMPLEMENTATION FOR FAMILIES: YOUR DIGITAL SECURITY ACTION PLAN

Just as your family likely has a plan for fire safety or natural disasters, it's time to create your family's digital security plan. Here's how to get started with two-factor authentication, broken down into manageable steps that won't overwhelm your household.

PRIORITY ACCOUNTS FIRST

Start with your most important accounts, like building a fence around your most valuable assets:

- Primary email accounts (they're often the recovery method for other accounts)
- Financial services (banks, credit cards, retirement accounts)
- Cloud storage (where you keep family photos and documents)
- Password managers (if you use one – and you should!)
- Social media accounts (especially if they contain family photos or private information)

SETTING UP 2FA: A FAMILY PROJECT

Pick a weekend afternoon to get everyone on board. Start by downloading an authentication app like Google Authenticator or Authy on each family member's phone. For younger children who don't have phones, parents can maintain their codes.

For each important account:

1. Log in and find the security or privacy settings
2. Look for "two-factor authentication" or "2FA" (sometimes called "two-step verification")
3. Follow the setup prompts, usually involving scanning a QR code with your authentication app
4. Save any backup codes provided in a secure location – think of these as your spare keys

BACKUP PLANS ARE ESSENTIAL

Just as you keep spare house keys with trusted relatives, create digital backup plans:

- Store backup 2FA codes in your family's fireproof safe or security deposit box
- Set up a recovery email address that belongs to another family member
- For physical security keys, keep a backup key in a secure location
- Write down step-by-step recovery instructions and store them with your other emergency documents

MANAGING FAMILY ACCESS

Consider what happens if someone is unavailable during an emergency:

- Keep a secure family document listing which accounts have 2FA enabled
- Ensure your spouse or trusted family member knows how to access critical accounts
- For shared family accounts (like Netflix or Amazon), decide who manages the 2FA verification
- Create an emergency access plan for your digital assets, just like you would for physical assets.

TEACHING MOMENT

Use this security upgrade as an opportunity to teach your children about digital responsibility. Explain how 2FA is like having a trusted adult verify their identity at school – it might take an extra moment, but it keeps everyone safe. This understanding will serve them well as they grow up in an increasingly digital world.

Remember, implementing better security is like building good habits – start small, be consistent, and eventually it becomes second nature. Your family's digital security is just as important as locking your doors at night or having a fire extinguisher ready. A small investment of time now can prevent significant heartache later.

See bio on page 11.



Photo by Vitaly Gariev on Unsplash

READY OR NOT READY:

EMERGENCY PREPAREDNESS QUIZ

Sourced from
the [US Navy](#)



You'll see emergency preparedness quizzes occasionally in the Journal of Civil Defense. Our goal is to ensure that you and your loved ones are prepared for any disaster that might occur. Please use these to familiarize yourself with what you should have ready, what you should know, and what you should do in the event of an emergency. We trust you'll become more and more prepared!

QUIZ

1. As long as I have all the necessary supplies for an emergency kit somewhere in my house, I am prepared for an emergency.
 - ☐ True
 - ☐ False
2. If local authorities told me to evacuate, I would:
 - ☐ Refuse to leave. Most 'emergencies' don't turn out to be a big deal.
 - ☐ Wait to see if the situation worsened, then decide.
 - ☐ Follow the advice of local responders to ensure my safety and theirs.
 - ☐ Call my neighbor and see what she thinks I should do.
3. Our emergency supply kit has enough materials to sustain myself and my family:
 - ☐ For at least four hours.
 - ☐ Through the night.
 - ☐ Until we get to a shelter.
 - ☐ For at least three days.
4. As long as one person in my family knows what our emergency plan is, our family is prepared.
 - ☐ True
 - ☐ False
5. My family and I have:
 - ☐ An emergency kit at home.
 - ☐ An emergency kit in the car(s).
 - ☐ An emergency kit at work.
 - ☐ All of the above.
6. Since my spouse is [in the military/an emergency personnel profession], he/she will be able to make sure our family is safe if an emergency strikes.
 - ☐ True
 - ☐ False
7. In terms of water, our emergency supply kit has:
 - ☐ A small bottle for each member of the family.
 - ☐ A gallon a day for each family member for three days.
 - ☐ One gallon for the family to share.
 - ☐ More water for the adults than the kids.
8. Our family's emergency plan contact person is:
 - ☐ Our next door neighbor.
 - ☐ Our family friend who lives two blocks away.
 - ☐ Grandma and Grandpa Smith who live in another state.
 - ☐ The Governor of our state.
9. The four aspects of being prepared for an emergency are:
 - ☐ Be informed, make a plan, build a kit, stay informed.
 - ☐ Call a friend, go to the hospital, go home, stand outside and watch.
 - ☐ Make a plan, practice the plan, keep the plan to myself, ignore the plan.
 - ☐ Water, batteries, map, perishable food.
10. Including children in the family emergency planning process will only scare them, so it should be avoided at all costs.
 - ☐ True
 - ☐ False

**Answer Key
on next page!**

ANSWER KEY

1. The correct answer is **False**. Keeping all of your emergency kit supplies stored all in the same location—preferably in a portable bag or container—will make it much easier to grab your kit and go in the case of an evacuation.
2. The correct answer is “**Follow the advice of local responders to ensure my safety and theirs.**” If local authorities advise you to evacuate, be sure to follow their instruction.
3. The correct answer is “**For at least three days.**” You may need to survive on your own after an emergency. This means having your own food, water, and other supplies in sufficient quantity to last for at least three days. Local officials and emergency personnel will respond after a disaster, but they may not be able to reach everyone right away.
4. The correct answer is **False**. If everyone in your family knows what your family emergency plan is and participates in developing the plan, nobody is left wondering what to do when an emergency strikes.
5. The correct answer is “**All of the above.**” Having kits in your home, your car, and at work will enable you and your family to respond to an emergency more quickly and will be useful whether you have to evacuate or shelter in place.
6. The correct answer is **False**. Due to the nature of being a [military/emergency personnel], your spouse may be deployed or called away to help others in the emergency situation, leaving you and your family left to react on your own.
7. The correct answer is “**A gallon a day for each family member for three days.**” In the event of a disaster, you may need to survive on your own for a period of time, so be prepared with enough water for everyone in your household for at least three days.
8. The most correct answer is “**Grandma and Grandpa Smith who live in another state.**” Your family’s emergency plan contact person should be someone who lives outside your region, preferably in another state. Otherwise, your contact person may be dealing with the same emergency situation and may be hard to reach.
9. The correct answer is “**Be informed, make a plan, build a kit, stay informed.**” The National Ready Campaign urges all Americans to be and stay informed about the potential disasters that could strike where you live, make an emergency plan, and put together an emergency supply kit.
10. The correct answer is **False**. When children are included in the family emergency planning process and know how to respond, it actually helps them stay much calmer in the event of an actual emergency situation.

Lava Gel Flame-Free Food Oven

Heat up to a total of 6 servings of food in this Lava Gel Oven Camping and Hiking Kit without fuel or fire! The Lava Gel Oven is able to heat a wide variety of food including freeze-dried, canned, home-made, or other prepared foods. Refrigerated or room temperature foods are heated to food safe temperatures in 7 to 12 minutes.



Available in the
TACDA Survival Store!



CLOUD SECURITY AND BEST PRACTICES



**By Bryson Meiling,
MS Business Entrepreneurship
and Engineering**

Your family photos, tax returns, and precious memories are probably in the cloud right now – but what exactly does that mean? If you're like most American families, you're using cloud services every day, from backing up phone pictures to storing important documents. Yet in an age where digital security threats are becoming more common, many of us aren't quite sure if our family's digital legacy is truly safe.

Think of the cloud like a digital safe deposit box - convenient, but only as secure as the key protecting it. Just as our grandparents taught us to be prepared and self-reliant, today's families need to understand how to protect their digital assets. The good news? You don't need to be a tech expert to keep your family's digital memories and documents secure.

UNDERSTANDING CLOUD BASICS

If you've ever shared photos from a family reunion through Google Photos, saved tax documents in Dropbox, or backed up your child's first steps video to iCloud, you're already using the cloud. But let's demystify what's actually happening behind the scenes. The "cloud" isn't some mysterious fog in the sky - it's a network of highly secure data centers where companies store your family's digital belongings.

Think of it like a modern, storage-unit facility. When you rent a storage unit, you're paying for space in a secure building that you can access whenever you need. Similarly, when you use cloud services, you're essentially renting digital space on someone else's secure computers. Your family photos aren't floating in space - they're stored on powerful servers, protected by the same kinds of security systems that guard our nation's largest banks.

The beauty of cloud storage is that it protects your family memories from local disasters like fires, floods, or computer crashes. It also means you can instantly share grandma's birthday photos with relatives across the country or access your emergency contacts list from any device. But just like you wouldn't leave your storage unit unlocked, your cloud accounts need proper security measures to keep your family's digital treasures safe.

COMMON THREATS TO FAMILY DATA

Just as we teach our children to be careful around strangers, we need to be vigilant about digital threats to our family's security. Today's cybercriminals aren't just anonymous hackers in dark rooms - they're sophisticated scammers who use clever tricks to gain access to your family's private information.

One of the most common threats is phishing, where scammers pretend to be legitimate companies or even family members to trick you into sharing passwords or clicking dangerous links. Imagine getting an urgent text that appears to be from your bank, or a convincing email that looks like it's from your child's school. These social engineering attacks prey on our trust and natural desire to help others or respond quickly to authority.

Ransomware is another growing concern for families. Criminals can lock up your precious photos and documents, demanding payment to restore access. One family in Ohio lost access to five years of baby photos and videos when their cloud storage was compromised through a suspicious email link. Identity thieves also target family cloud accounts, knowing they contain tax returns, medical records, and other sensitive documents that could be used to steal your family's identity or financial information.

But don't let these threats overwhelm you. Just as we install security systems in our homes and teach our kids

about stranger danger, there are straightforward steps every family can take to protect their digital lives. The key is knowing what to look out for and having a family plan for responding to suspicious activity.

ESSENTIAL SECURITY PRACTICES

Protecting your family's digital life doesn't require a degree in computer science. It just takes implementing a few key habits. Think of these practices like the basic safety rules we all follow: locking our doors, having a fire escape plan, and keeping emergency contacts handy.

First, let's talk about passwords - your digital front door. Using "password123" or your anniversary date is like leaving your key under the doormat. Instead, use a password manager. Think of it as a secure digital safe that creates and remembers strong passwords for all your accounts. Popular options make this surprisingly simple, and you can even share certain passwords securely with family members while keeping others private. My personal recommendations are password managers like Password1 (<https://1password.com>) or Bitwarden (<https://bitwarden.com>); the password managers built directly into iPhones and Samsung phones are also good.

Two-factor authentication (see "Two-Factor Authentication & Why You Need It" on page 20) is your second line of defense - like having both a deadbolt and an alarm system. When enabled, even if someone gets your password, they'll need a second verification (usually a code sent to your phone) to access your accounts. Yes, it takes an extra few seconds, but those seconds could prevent your family photos and sensitive documents from falling into the wrong hands.

Finally, follow the 3-2-1 backup rule: keep three copies of important family data, store them on two different types of storage (like the cloud and an external hard drive), and keep one copy off-site. This way, if something happens to one backup, you'll still have access to your important memories and documents.

TEACHING KIDS ABOUT CLOUD SAFETY

Just as we teach our children to look both ways before crossing the street, we need to guide them in navigating the digital world safely. Today's kids are growing up in a world where sharing photos and storing schoolwork in the cloud is as natural as breathing. Our job isn't to frighten them about technology, but to empower them with good habits and sound judgment.

Start with the basics: teach kids that digital items, like family photos and documents, are valuable and private - just like the special items we keep in a physical safe at

home. Help them understand that some things are okay to share (like a family vacation photo), while others should remain private (like their full name or address). Make it a family activity to regularly review cloud sharing settings together, especially for apps and games they use.

Create clear family guidelines about what can be stored in the cloud. For younger children, this might mean having a shared family cloud account that parents monitor. For teens, it could involve a gradual introduction to managing their own accounts while following family safety rules. Consider setting up regular "digital safety chats" during family dinners, where you can discuss new apps, recent scam attempts, or concerns about online activities. Remember, we're not just teaching cloud safety, we're teaching responsibility, critical thinking, and the importance of protecting what matters. When kids understand the 'why' behind digital security, they're more likely to make smart choices even when we're not watching over their shoulders.

EMERGENCY PREPAREDNESS IN THE DIGITAL AGE

As Americans who value self-reliance and preparedness, we know the importance of having emergency plans for our families. Today, that means having both a physical and digital emergency kit. Just as we store essential supplies and important documents in a waterproof container, we need a secure digital vault for our critical information that's accessible when disaster strikes.

Start by creating a secure, digital, emergency folder in your cloud storage. This should include scanned copies of birth certificates, insurance policies, medical records, and emergency contacts. Make sure multiple trusted family members know how to access these documents, even if cell networks are down. Consider storing offline copies of access instructions in your physical emergency kit - sometimes old-school backup plans are still the most reliable.

Remember to regularly update your digital emergency preparations, just as you rotate your emergency food and water supplies. Set a quarterly reminder to verify that all your cloud backup systems are working, passwords are current, and emergency contacts are up to date. Pay special attention to maintaining offline copies of your most critical documents; during a natural disaster, internet access isn't guaranteed.

This balanced approach - combining traditional emergency preparedness with modern cloud storage - ensures your family can access vital information whether facing a power outage, natural disaster, or cyber incident. It's

about adapting time-tested principles of preparedness to protect our families in today's digital world.

PRACTICAL TIPS FOR IMPLEMENTATION

Securing your family's digital life doesn't have to be overwhelming. It's about building simple, consistent habits that become as natural as checking the locks before bedtime. Start with a weekend "Digital Security Saturday" to get your family on track. Gather everyone around the kitchen table and make it a family activity: check and update passwords, verify backup settings, and review sharing permissions on your cloud accounts.

Create a monthly maintenance routine that becomes part of your family's regular schedule, like checking the smoke detector batteries or rotating emergency supplies. Set aside 15 minutes on the first Sunday of each month

to:

- Review any suspicious account activities
- Update emergency contact information
- Check that cloud backups are working properly
- Discuss any new apps or services the family is using

Remember, the goal isn't perfection - it's progress in protecting what matters most. Just as our grandparents taught us the value of preparedness and self-reliance, we're teaching the next generation how to be responsible digital citizens. By taking these simple steps today, you're not just securing your family's memories and documents; you're creating a legacy of digital responsibility that will serve your family for generations to come.

See bio on page 11.

Dr. G. Landon Beales | TACDA Advisory Board Member

In Memoriam



We are deeply saddened by the passing of Dr. Landon Beales, a cherished member of our Advisory Board. Landon offered unwavering support and invaluable contributions to The American Civil Defense Association for many years. His dedication, wisdom, and passion helped shape our mission and impact countless lives.

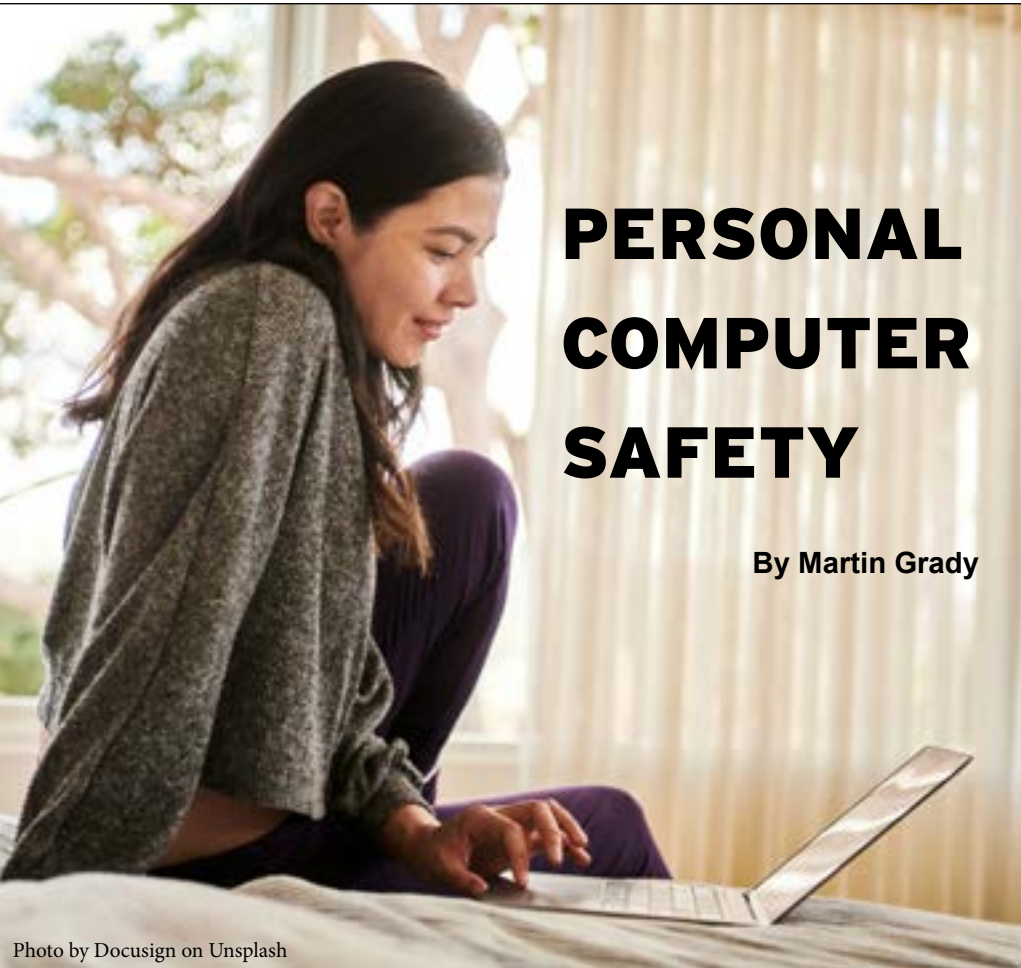
An Honorable Man and a Wonderful Life Well Lived

Encouraged by his mother, Landon pursued medicine and graduated from the University of Utah Medical School. He specialized in Internal Medicine and was known for his humility, compassion, and dedication to his patients. Landon had a wide range of interests and hobbies. He was an accomplished violinist, photographer, and amateur "ham" radio operator. He was actively involved in the Boy Scouts of America, raising five sons who all achieved Eagle Scout status. He was skilled in automobile mechanics, emergency preparation, and much more. Landon could fix anything, and if he didn't know how, he learned.

Landon loved exploring, going on off-road four-wheeling adventures, and discovering the beauty of the outdoors everywhere he could in Utah. His love for the outdoors extended to scuba diving, archery, snow skiing, camping, and hiking, with Lake Powell being a favorite destination for family time. Landon's biggest passion, however, was his family. Landon created a Legacy of Love for his posterity. He always had a kind word for everyone. He was a man of character, love, compassion and humility.

Landon's devotion and love of the scriptures and the gospel of The Church of Jesus Christ of Latter-day Saints was a guiding light throughout his life, providing him with strength, direction, and a deep sense of purpose. His favorite calling was teaching the Gospel Doctrine class, which he excelled at for over 25 years.

Landon's legacy of service and commitment will always be remembered and honored, and we extend our deepest gratitude for his remarkable influence on our organization and the community we serve. Landon will be greatly missed. His love and teachings continue to live on within all who had the privilege of knowing him.



PERSONAL COMPUTER SAFETY

By Martin Grady

Photo by Docusign on Unsplash

The world has witnessed widespread adoption of “smart” devices in the past couple decades. The ubiquity of the mobile phone has caused many to rely less on their personal computer for completing tasks and communicating. However, if you value your personal privacy, a home computer offers much higher security than a mobile device—provided that you take the proper precautions.

Before you can practice good cybersecurity, you must ask yourself what kind of privacy matters to you. Consider the following:

1. An AT&T technician named Mark Klein revealed, in 2006, that the National Security Agency (NSA) operates telecommunications interception facilities throughout the United States. Imagine that you live in an apartment building, and someone has installed a “cable splitter” on the line running to your house, allowing them to watch cable TV on your account. The NSA runs fiber optic beam splitters in the back rooms of these telecom companies which allow the agency to parse the incoming signal in the same way—except in this case, they’re tapping backbone

traffic to gain access to virtually all internet communications.

2. In 2013, that same agency opened a massive data center in rural Utah where it stores the mass of data it collects as part of its beam-splitting program. While the NSA claims this facility is simply for storage, the center experienced several power surges and fires since its completion and currently uses almost two million gallons of water a day to prevent overheating. This strongly suggests massive amounts of data processing and not just storage. One possible use for all this processing is mass decryption of encrypted data. Another is to train artificial intelligence; however, the public doesn’t know for sure and the NSA does not disclose this.
3. In 2006, British mathematician Clive Humby coined the phrase “data is the new oil” to describe the potential value of the masses of data increasingly siphoned from the public. We have seen, in the years

following this declaration, a “gold rush” of personal data extracted from society and sold to all kinds of interested parties. Consider that if a corporation can acquire your data to sell you products, so too can a think tank use our information to sell us ideas. We may like to believe we are immune to propaganda, but even the most skeptical among us may become susceptible to manipulation by think tanks or propagandists empowered with algorithms that may, in some ways, understand us better than we even know ourselves.

With this in mind, and while recognizing that it may be impossible to achieve perfect privacy in the current environment, let’s look at a few things you could do to protect your data.

USE OPEN-SOURCE SOFTWARE

Most commercial software is “closed-source”. This means that the code which powers the software is encrypted or otherwise unavailable to review or modify. If a program was written insecurely, or even intentionally equipped with back doors to allow intrusion or to leak your data, the public would have no way to detect or verify this without being able to browse the source code.

However, well-maintained, open-source software is auditable, and with lots of eyes on potential security flaws, it is often more secure as well.

I run **Linux** as the operating system on all my computers, which is completely free and open-source. I use a version of Linux called Ubuntu, and I think this is the most user-friendly Linux distribution. You can [download Ubuntu](#) and run it from a thumb drive, as a demo, and then install it on your hard drive if you decide it's right for you. When I started using Linux almost 20 years ago, I had a dual-boot computer which would let me choose either Ubuntu or Windows. Once I became familiar enough with Linux, I ditched Microsoft and have never looked back.



Be aware that Linux has a learning curve, compared to Windows or MacOS; however, once you become familiar with the OS, you'll find it can accomplish all the basic tasks of a Mac or Windows PC. You won't need to run antivirus software because your operating system will be virtually impervious to viruses. Linux runs surprisingly well on machines with old or outdated resources, so your last Windows machine may be a perfect candidate for your first Linux one.

Almost all the other programs available to install on Linux are also free and open-source, but:

USE YOUR OWN HARDWARE TO CONNECT TO THE INTERNET

Your Internet service provider will usually send you a proprietary combination modem/router when they install your service. Usually, they consider this a "lease", and they view the hardware as their property, not yours. Even if they don't, this device is proprietary and closed-source, calling into question its security and respect for your privacy. Luckily, you can buy your own router and use this with your service, and there is open-source, Linux-based software to power routers as well. I use OpenWRT which supports several devices (see which ones at https://openwrt.org/supported_devices). I have also used ddwrt (<https://dd-wrt.com>) in the past.

You can access the firmware for these routers using a web interface, where you have granular control over who can be on your home network and what can be accessed. You can review the event logs to analyze the traffic on your network, turn wi-fi on and off on a schedule, and even install an ad-blocker at the router level which will block all ads and ad trackers from every device in your home.

USE A PASSWORD MANAGER

If you could make a single first step to protect your security while on your computer, I would recommend using a password manager. It's not worth trying to remember a million passwords, and if you're using the same password over and over then a single leaked or insecure password could expose all your logins to a would-be intruder. A password manager stores all your passwords for you so that you don't have to remember any of them. Just let the program generate a long, unbreakable password, and when you need to use it, just copy it from the program and paste it into your password field. I have used [KeePassXC](#) for years, which is available on Linux, Mac and Windows. There's even a portable KeePass (<https://keepass.info/download.html>) for Windows that you can run from a thumb drive, if you want. Avoid cloud-based software when possible.



There are plenty of online password management solutions, but then you're entrusting all your sensitive passwords to live on a server somewhere on the Internet. A lot of software companies have been shifting to a software-as-a-service model, where you don't physically possess or control the software on your own machine. The less of your data you can keep floating around on the internet, the better. My family uses Nextcloud (<https://nextcloud.com>) on our home network—an open-source

EMP-Resistant Waterproof USB

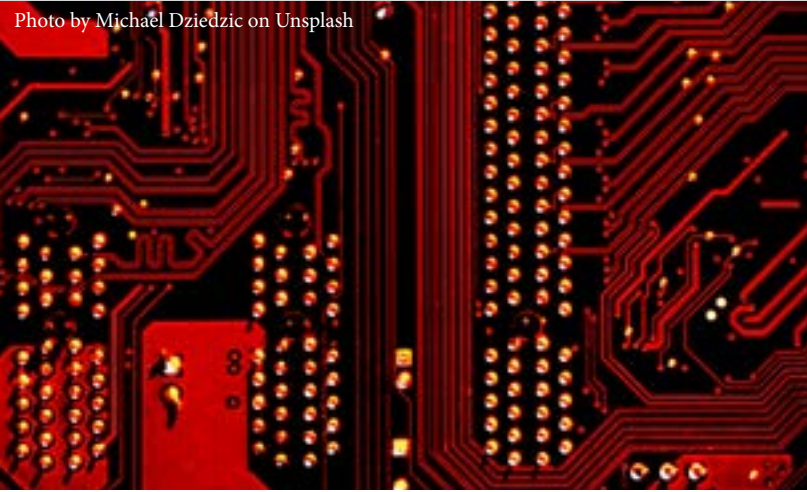
Pre-loaded with all of the TACDA emergency resource essentials!



Available in the
TACDA Survival Store!



Photo by Michael Dzedzic on Unsplash



solution that replaces a lot of the services offered by Dropbox and Google Office Suite. If you're in the habit of emailing a note to your spouse who's sitting in another part of the house, consider that the computers in your home can talk to each other without sending those communications out into cyberspace.

In review, there are two things you can try today to improve your security when on your home computer:

- Use a password manager; and
- Use open-source software that resides on your local machine, when possible.

These two steps should go a long way toward safeguarding your information. Recognize that almost any information you pass over the internet—even encrypted information—can be intercepted. If your data is stored indefinitely, then even encryption that's unbreakable today may not be in the future. You could even consider having a dedicated machine at home that you keep disconnected from the Internet, which is the most reliable way to keep your data offline. But the actual first step to home computer security may be a philosophical one. Think about what it means to own your data, to own your software, and the “unknown unknowns” of sharing your data.

The current proliferation of AI-powered tools that have debuted in the last couple years threaten the livelihoods of artists, copywriters, and an untold number of other professions. These tools can only exist because they are trained on the massive amount of data that the public has surrendered for the convenience of “free of charge”, online-based tools for which virtually none of us have read the small print. Surely, very few of us considered that we may be training AI to make us redundant when we gave up our data, many assuming, blithely, that they have no reason to worry because they're not “doing anything wrong”. Hopefully we can become savvier as a society, moving forward.

Will you remember what to do after a nuclear attack?

NUCLEAR DETONATION SURVIVAL CARD

NUCLEAR DETONATION SURVIVAL CARD

- A.** Drop and cover when you see a flash. Stay behind the cover for two full minutes. Even covering with paper can prevent burns. Keep your eyes closed during bright light to prevent blindness.
- B.** 7/10 Rule: Fallout loses 90% of its radioactivity in the first 7 hours after a detonation and an additional 90% for every 7-fold increase in time: 90% in the first 7 hours, 99% in 49 hours (2 days), and 99.9% in two weeks.
- C.** Fallout looks like sand, ash or grit as it falls and accumulates on the ground. If no fallout is visible on the ground, there is no radiation! To be sure, place a piece of white paper, or anything with a smooth surface on the ground & check every 15 minutes for fallout particles.

FRONT

KNOWING A, B, & C, CAN SAVE YOUR LIFE

If visual indications of fallout appear, take shelter for two or three days underground or behind thick walls.

Give a card to each emergency responder in your jurisdiction and share it with the general public.

These principles were developed during nuclear weapons tests from the 1940's – 1960's and remain valid today! The laws of physics do not change.

This card presented by: PhysiciansForCivilDefense.org

Courtesy of The American Civil Defense Association
(TACDA) www.tacda.org

BACK

Stay prepared and informed in case of a nuclear emergency with this **wallet-sized instruction card** for nuclear detonation, blast, fallout, and radiation protection and survival.

Available in the TACDA Survival Store!



TACDA

PO BOX 1003
Sandy, UT 84091
www.tacda.org
info@tacda.org
Office: (800) 425-5397
Fax: (801) 662-0367
ISSN: 0740-5537



The American Civil Defense Association is on Facebook!
Take the time to LIKE us and receive more valuable links and updates!

Disclaimer Notice

Please read this disclaimer carefully before reading the Journal of Civil Defense, created by The American Civil Defense Association (TACDA). The content displayed in this journal is the intellectual property of The American Civil Defense Association. You may not reuse, republish, or reprint such content without our written consent. All information posted is merely for educational and informational purposes. It is not intended as a substitute for professional advice. Should you decide to act upon any information in this journal, you do so at your own risk. The content displayed in this journal and the opinions of the authors do not necessarily agree with the purposes, policies, or beliefs of The American Civil Defense Organization, our executive directors, our editors, our advisors, or our board of directors. While the information on this website has been verified to the best of our abilities, we cannot guarantee that there are no mistakes or errors. We reserve the right to change this policy at any given time, of which you will be promptly updated. If you want to make sure that you are up to date with our latest policies, we advise you to frequently visit our website at www.tacda.org.

Together we are stronger! Join us!

The mission of The American Civil Defense Association is to empower and equip individuals, families, and communities through educational means to be prepared for emergencies and disasters.

Become a member now and receive information and resources to better understand current threats and practical solutions for handling emergencies.

www.TACDA.org

TACDA™ is a registered 501(c)3 non-profit, non-political organization.
Donations are always appreciated.

TACDA MEMBERS RECEIVE:

A FREE E-JOURNAL OF OUR
BI-ANNUAL PUBLICATION,
THE JOURNAL OF CIVIL DEFENSE

ACCESS TO READ, BUY, AND/OR
DOWNLOAD ALL BACK ISSUES
OF THE JOURNAL OF CIVIL
DEFENSE ARCHIVES FROM 1968

ACCESS TO THE TACDA
ACADEMY AND OTHER MEMBER
RESOURCES

MEMBER DISCOUNTS ON
PRODUCTS AND SERVICES
THROUGH THE TACDA STORE

HARD-COPY SUBSCRIPTIONS TO
THE JOURNAL OF CIVIL
DEFENSE ARE NOW AVAILABLE
FOR \$15/YEAR!