



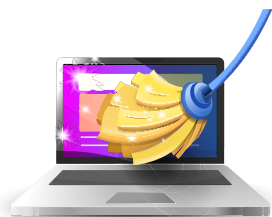
**PROJECT
CYBERSAFE™**

NEWSLETTER

A QUARTERLY PUBLICATION FOR NSSF AND SAAMI EMPLOYEES

DIGITAL SPRING CLEANING

Digital spring cleaning refers to the clean-up and organization of your devices and online accounts. Your digital life can quickly become cluttered and disorganized. This includes your computer, phone, email, social media accounts, and other digital assets. These digital hygiene practices can protect your digital assets from cybercriminals.



Reviewing your subscription services can help you identify services you no longer need and save money every month.

SECURITY CHALLENGES CREATED BY AI

AI making phishing attacks more dangerous isn't the only AI security risk to your business. This TechTarget article highlights 6 security challenges along with best practices to mitigate risk for your business as the adoption of AI increases.

Having an AI Policy in place is the best first step to making sure your business doesn't find itself facing these security challenges posed by AI. [Read more...](#)



KIDS CORNER

The Family IT Guy has 3 great tips for parents on how to teach your kids about AI

1. **NO** using AI alone.
2. **NO** pretending AI is a person.
3. **NO** outsourcing their thinking.

Watch his explanation about each tip on his YouTube channel [here](#).



GOING TO THE SOURCE

Going to the source website is the best course of action when interacting with your bank, email, shopping or business logins. Relying on a link from an email or text message puts you at risk for giving your credentials away to cybercriminals. This [KnowBe4 blog article](#) provides advice on how to further protect yourself such as treating surprise 'extra security' prompts after a failed login with caution, especially if they ask for answers to security questions, card numbers, or email passwords.

MODERN SOCIAL ENGINEERING WITH DEEPFAKES

The news cycle has highlighted that urgency isn't just a worry in your day to day work world. It extends to every part of our life. This [KnowBe4 article](#) discusses the danger of rushing to be the first to know or the first to report.

"The takeaway for organizations and individuals is clear: visual content can no longer be trusted at face value, especially during fast-moving events. Training people to pause, question sources and look for verification is just as important for news consumption as it is for email security."



BRAND IMPERSONATION ON THE RISE

Brand impersonation is a threat to your organization that continues to find its way into your employee's inbox. This [Guard.io article](#) details the most impersonated brand for Q4 2025.

To ensure your business is as secure as possible, test your employees with simulated phishing tests and provide them with security awareness training on the newest techniques used by cybercriminals.

KnowBe4 is a Member Benefit for NSSF Members. Contact them today and they can provide a package that works best for your business [Click this link for the NSSF members KnowBe4 offer](#).

A PROGRAM OF
NSSF
The Firearm Industry
Trade Association

Review your business's cybersecurity posture in these 11 categories and see where you can make improvements to make your business more secure. Visit the NSSF Member Portal for more cybersecurity resources only available to NSSF Members. If you have any suggestions on future topics for us to cover, please email us at projectcybersafe@nssf.org.

GOOD | BETTER | BEST



PASSWORDS	AUTHENTICATION	WIFI
GOOD Never share credentials	GOOD Multifactor Authentication	GOOD Changing the router's default password
BETTER Never reuse a password	BETTER Multifactor Authenticator App	BETTER Segmenting the Wi-Fi so that only approved devices are on the secure Wi-Fi network and non-approved devices are public.
BEST Using a password manager to create unique complex password	BEST Utilizing PassKey technology	BEST Hiding your network or using encryption methods like WPA3 to prevent unauthorized access.
POLICIES	PHISHING AWARENESS	INCIDENT RESPONSE
GOOD Have clearly defined data use and security policies.	GOOD Monthly phishing email tests and Quarterly awareness training	GOOD Developing an effective plan.
BETTER Review and update your policies	BETTER Weekly phishing email tests and Monthly awareness training	BETTER Periodic review of the plan and revise as necessary.
BEST Test your policies and procedures	BEST Continuous phishing email tests and Monthly awareness training	BEST Testing the plan and incorporating the lessons learned.
CYBERSECURITY DEPENDS ON EVERYONE		
AUDITS	BACKUPS	
GOOD Regular internal and external security audits.	GOOD Automated Backup Systems (follow the 3-2-1 backup rule)	
BETTER Security Information and Event Management for real-time alerts.	BETTER Testing and verifying data on a regular basis.	
BEST Establishing a penetration testing schedule for your internal and external assets.	BEST Develop a comprehensive data recovery plan so that it's fully documented.	
PATCHING (PC)	PATCHING (SERVER)	MOBILE SECURITY
GOOD Enable Auto Updates for Operating System	GOOD Monthly OS patching schedule	GOOD Turn ON Screen lock and turn OFF lock screen notifications
BETTER Enable Auto Updates for your software Apps	BETTER Test environment for patching prior to pushing out to production environment	BETTER Only download apps from approved App stores and ensure your operating system and Apps are up to date
BEST Automated Patch Management Software	BEST Automated vulnerability and patch management solution that patches your other software Apps as well as your Operating System.	BEST Mobile Device Management, remote wipe, managed apps and updates