PROJECT CYBERSAFE™ NEWSLETTER

A QUARTERLY CYBERSECURITY PUBLICATION FOR THE FIREARMS INDUSTRY

CLICKFIX SOCIAL ENGINEERING IS NOW THE LEADING MALWARE DELIVERY METHOD

ClickFix attacks are a new trend where cybercriminals try to trick an end user into copying, pasting and running malicious code on their computer by pretending to fix and error or CAPTCHA prompt. These attacks have been so successful that they are now the leading malware delivery method.

It is critical that you keep your employees up to date on these new attacks by cybercriminals to protect your business from disruption of service or loss of income.

knowbe4

KnowBe4 is a member benefit to NSSF Members and would be happy to get your company aligned with a package that will best serve your employees and business. Click here for more information.

WARNING—

COMPROMISED HOTEL ROUTERS SEND USERS TO PHISHING SITES

Employees that travel are being attacked by a DNS poisoning attack on hotel Wi-Fi routers. (From KnowBe4 Blog) This campaign is particularly dangerous because the victims aren't targeted with suspicious emails; they're simply presented with a legitimate-looking Microsoft 365 login page. The phishing sites are also designed to intercept OAuth tokens, granting the attacker access to the account after the user approves a prompt.

REPORT—

VISHING AND DEVICE CODE PHISHING ARE SURGING

The 2026 Threat Hunting Report from CrowdStrike (Project CyberSafe Partner) highlights how social engineering continues to be a central part of modern cyberattacks. During the 1st half of 2026 Voice Phishing has shown a 2x increase in intrusions, while device code phishing attacks have increased by 15x. Having a security awareness program for your business will strengthen your security culture and reduce workforce risk. **Read the CrowdStrike 2026 Threat Hunting Report here.**

AI QUICK GUIDE

NSSF® Project CyberSafe™ has created their 1st Quick Guide around the topic of AI Policy, Evaluation and End User guidance to help members with an easy to digest document to assist with simplifying the onboarding of Artificial Intelligence products. Click here to access the NSSF AI Quick Guide.

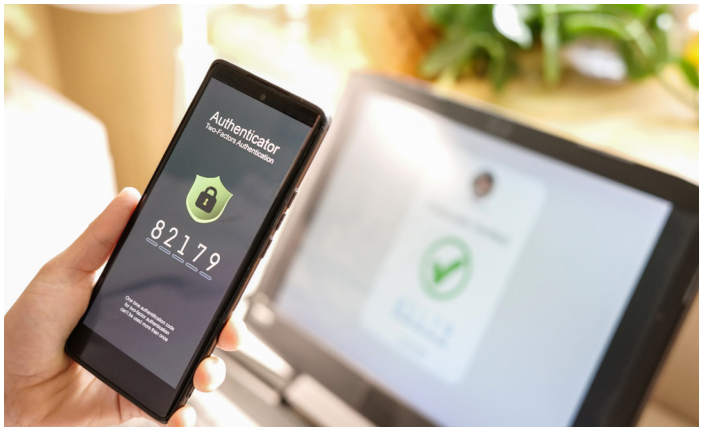
OCTOBER IS CYBERSECURITY AWARENESS MONTH

Cybersecurity Awareness Month is an international initiative that educates everyone about online safety and empowers individuals and businesses to protect their data from cybercrime.

The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance co-lead the campaign and create resources for organizations to talk to their employees and customers about staying safe online.

You can request a Cybersecurity Awareness ToolKit from the National Cybersecurity Alliance here.

You can get a FREE RESOURCE KIT from KnowBE4 with 4 weeks of materials here.



REPORT—

PHISHING REMAINS THE PRIMARY INITIAL ACCESS VECTOR

This Incident Response trends article from Cisco Talos reminds us that Phishing remains the primary initial access vector. They have also seen a spike in authentication abuse using methods such as MFA fatigue attacks to gain access to accounts.

Make sure you have MFA enabled on every software your company uses and educate your employees about the importance of not falling for MFA fatigue attacks.

CYBERSECURITY NETWORKING EVENT AT SHOT SHOW® 2027

Since its inception in 2023, NSSF's Project CyberSafe™ has provided cybersecurity-related guidance, information and best practices to the firearms industry. To date, this has taken shape as surveys, webinars and industry roundtables — as well as the Project CyberSafe website, email campaigns and newsletters.

More importantly, we have built relationships throughout the industry to leverage your expertise, share our approaches and solve the industry's problems together.

As we head into 2027, we are looking at how best to serve the industry through Project CyberSafe. Your thoughts and input would be invaluable.

NSSF will be hosting a networking event with our cybersecurity advisor Fellsway at SHOT Show® 2027. We aim to create some new relationships and brainstorm ways to further Project Cybersafe as we look to the future. For more information, please email projectcybersafe@nssf.org