NMFTA CORE CYBERSECURITY CONTROLS CHECKLIST

Protect Yourself and Your Business as an Owner Operator

Cybersecurity is not high on the list of concerns for many owner operators. Much of the time your entire technical infrastructure consists of your phone, your laptop and/or a tablet, and your truck. It's easy to feel that it's highly unlikely that you will become a victim of a cyberattack. Unfortunately, that is a false sense of security. Threat actors indiscriminately scan thousands of random people and devices every day looking for targets of opportunity. Once they identify a weakness, they will find an angle to try to make a quick buck, seeking to blackmail you, drain your bank account, encrypt your files for a ransom payment, or steal your identity to resell elsewhere. While this level of threat can seem overwhelming, the good news is that there are many straightforward, low-cost and even free measures that can be taken to avoid becoming an easy target for these criminals.

This checklist outlines core cybersecurity controls that can simply be put in place and provides easy to follow steps you can take to dramatically increase your level of cybersecurity without breaking the bank. These controls can serve as the backbone of your cybersecurity practice whether you are a solo operator with one power unit, or you are looking to scale your business up to bring on more power units and more employees. Cybersecurity is as much of a mindset as it is a technical practice. Adopting a defensive approach and minimizing unnecessary risks will make you significantly more secure and better prepared to face the reality of cybersecurity threats to your business.

NMFTA™
National Motor Freight Traffic Association, Inc.

CYBER

LIMITED USE LICENSE. NMFTA hereby grants a non-transferable, non-exclusive, limited license to use this document solely for your own internal use and benefit only. Except as expressly permitted in writing by NMFTA or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means, this document and its contents in total or in part. Reverse engineering, disassembly, or decompilation of this document, unless required by law for interoperability, is prohibited.

PRIVACY. This Limited Use License is subject to the terms and conditions of NMFTA's Privacy Policy ("Policy"), (Privacy Policy - NMFTA - National Motor Freight Traffic Association) where we describe how the National Motor Freight Traffic Association, Inc. ("NMFTA") collects, uses, and discloses information that we obtain about visitors to our website nmfta.org, including any related sites that share the same or similar branding (the "Site") and the services available through our Site (collectively, the "Services"). By visiting the Site and downloading the NMFTA Core Cybersecurity Controls Checklist, you agree that your personal information will be handled as described in this Policy. Your use of the downloaded document and the NMFTA Site or any Services, is subject to this Privacy Policy and NMFTA's Terms of Use, including its applicable limitations on damages. The NMFTA Terms of Use are incorporated by reference into this Limited Use License.

Secure All Business and Personal Accounts with Strong, Unique Passwords

- [ ] Unique passwords for every account. Use a password manager to store credentials securely and avoid re-use.
- [ ] Make sure that your passwords are at least 12 characters long and include a mix of upper- and lower-case letters, numbers, and symbols.

Enable Multi-Factor Authentication (MFA)

- [ ] Adds an additional layer of security if one of your passwords is compromised.
- [ ] Prioritize MFA for any account handling sensitive information, like banking or credit card portals.
- [ ] Use an authenticator app instead of an SMS or text code if possible.

Keep All Software and Firmware Up-to-Date

- [ ] Keep your phone, laptop, and all other electronic devices updated with the latest security patches.
- [ ] Enable automatic updates on mobile phones, tablets, and laptops.
- [ ] Remember to update apps and software that you install on these devices too.
- [ ] Be aware of social engineering scams
- [ ] Scammers often target owner operators with fake invoices or payment requests, or links to fake load boards.
- [ ] Verify all emails and text messages that claim to be from customers, brokers, or financial institutions.
- [ ] Never share account details or sensitive information unless you are 100% confident of the other party's legitimacy.

Monitor Credit and Financial Accounts

- [ ] Sign up for credit monitoring services to detect fraudulent attempts to use your credit.
- [ ] Regularly review all bank and credit card statements for any suspicious charges. Freeze your credit any time you are not planning to open new accounts or take out loans.

Secure Wi-Fi Connections

- [ ] Avoid using public Wi-Fi networks at truck stops or rest areas unless you are connected through a virtual private network (VPN).
- [ ] Set up a secure hotspot on your phone or tablet for private connections.
- [ ] Change default passwords on your home or in-truck Wi-Fi router and enable WPA3 if available.

Backup Business Data

- [ ] Backup important documents such as receipts, invoices, permits and contracts to a secure cloud storage service or encrypted external drive.
- [ ] Schedule automatic backups on your devices to reduce the risk that critical data is lost.
- [ ] Remember the 3-2-1 rule: Three copies of your data, in two different forms with at least one copy stored offsite.

Minimize Personal Information Exposure

- [ ] Be cautious about sharing personal or business details online, including U.S. Department of Transportation (USDOT) numbers, license numbers, and load details.
- [ ] Use privacy settings on social media to restrict access to personal posts.
- [ ] Regularly check your USDOT or motor carrier (MC) numbers on Federal Motor Carrier Safety Administration's (FMCSA's) site and public directories to ensure that they have not been fraudulently misused.

Use Reliable Security Software

- [ ] Install antivirus and anti-malware tools on all of your devices, including phones, tablets, and laptops.
- [ ] Use software that offers real-time protection against ransomware, spyware, and other threats.
- [ ] Keep your antivirus and anti-malware software updated.

Secure Mobile Devices

- [ ] Lock devices with pins, patterns, or biometrics.
- [ ] Require biometric authentication to access sensitive apps.
- [ ] Configure auto-lock for all devices and restrict physical access to devices when not in use.

VISIT NMFTA.ORG/CYBERSECURITY FOR MORE RESOURCES

1001 N. Fairfax Street, Suite 600
Alexandria, VA 22314-1798
(866) 411-6632
www.nmfta.org