

# Happy New Year 2021

January-February 2021 | Issue 2021:1



## CSO's Message

Welcome 2021!

The new year gives us a chance to review, reflect and reboot. This issue contains information to reinforce your digital security. DTI is committed to 24/7 security for our state network. It is our duty to protect Delawarean's private information while continuing to offer the online services that are more important than ever.

Solomon Adote  
Chief Security Officer

## Digital Security Priority Actions



**Do these quick check ups and secure your online activity in 2021!**

**Manage Passwords** Complicated passwords keep the bad guys out and you need a different one for each account. Password Manager applications make this easier by saving passwords and entering them when you log in. You only have to remember one master password for the application to let it manage your passwords for you. See more information at [Cyber Security Resources on our DigiKnow website.](#)

**Multi-Factor Authentication** Use Multi-Factor Authentication (MFA) — aka two-factor (2FA), whenever and wherever possible. Both Microsoft and Google have recently stated that MFA will stop 99 percent of all automated attacks.

**Virtual Private Networks (VPN)** A VPN encrypts your Internet connection to secure it and protect your privacy. You can select "no sharing" to further protect information. Most smart phones and many devices offer this option. [The Best Free VPNs for 2021 | PCMag](#)

## Protect Your Privacy Online!



**Facebook Privacy Checkup** Manage who can see your stuff! Click the downward arrow button in the upper right corner of your Facebook page. Then click on "Settings & Privacy" and "Privacy Checkup". This easy-to-use wizard will guide you through settings that will enable you to lock your profile so that only your friends can see it — and scammers will be locked out. [Read more about Facebook privacy.](#)

**Smart Devices** When setting up smart devices, always change the default password. Most of these devices work from your wireless router, so password protecting your Wi-Fi can also help. Keep up with firmware updates; many devices will inform you when there's an update available. You may want to allow your device to accept manufacturer operating system updates automatically. Also look for an "Update Firmware" option.

**Bluetooth** If you leave your Bluetooth on in public places after using a hands-free headset, hackers can easily connect to your phone, manipulate it, and steal your data. Make it a habit: always turn Bluetooth off after you use it. Set your visibility to "off" or "not discoverable," and require a security code when your device pairs with another Bluetooth device.

[Read more Cybersecurity News at DigiKnow!](#)



Delaware Department of Information & Technology publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to <https://digiknow.dti.delaware.gov>.



Department of Technology and Information  
Contact us at [esecurity@delaware.gov](mailto:esecurity@delaware.gov)

