# BLUE|LINE

# Cybersecurity Recommendations

**1. Change Passwords and Use Strong Passwords:**

- The number one reason systems get "hacked" is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible.A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

**2. Update Firmware**

- As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

**"Nice to have" recommendations to improve your network security**

**1. Change Passwords Regularly**

- Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

**2. Change Default HTTP and TCP Ports:**

- Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

**3. Enable HTTPS/SSL:**

- Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

**4. Enable IP Filter:**

- Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

**5. Change ONVIF Password:**

- On older IP Camera firmware, the ONVIF password does not change when you change the system' s credentials. You will need to either update the camera' s firmware to the latest revision or manually change the ONVIF password.

**6. Forward Only Ports You Need:**

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

**7. Disable Auto-Login on SmartPSS:**

- Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

**8. Use a Different Username and Password for SmartPSS:**

- In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system

**9. Limit Features of Guest Accounts:**

- If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

**10. UPnP:**

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

# BLUE|LINE

# Cybersecurity Recommendations

**11. SNMP:**

● Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only

**12. Multicast:**

● Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

**13. Check the Log:**

● If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

**14. Physically Lock Down the Device:**

● Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key

**15. Connect IP Cameras to the PoE Ports on the Back of an NVR:**

● Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

**16. Isolate NVR and IP Camera Network**

● The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.