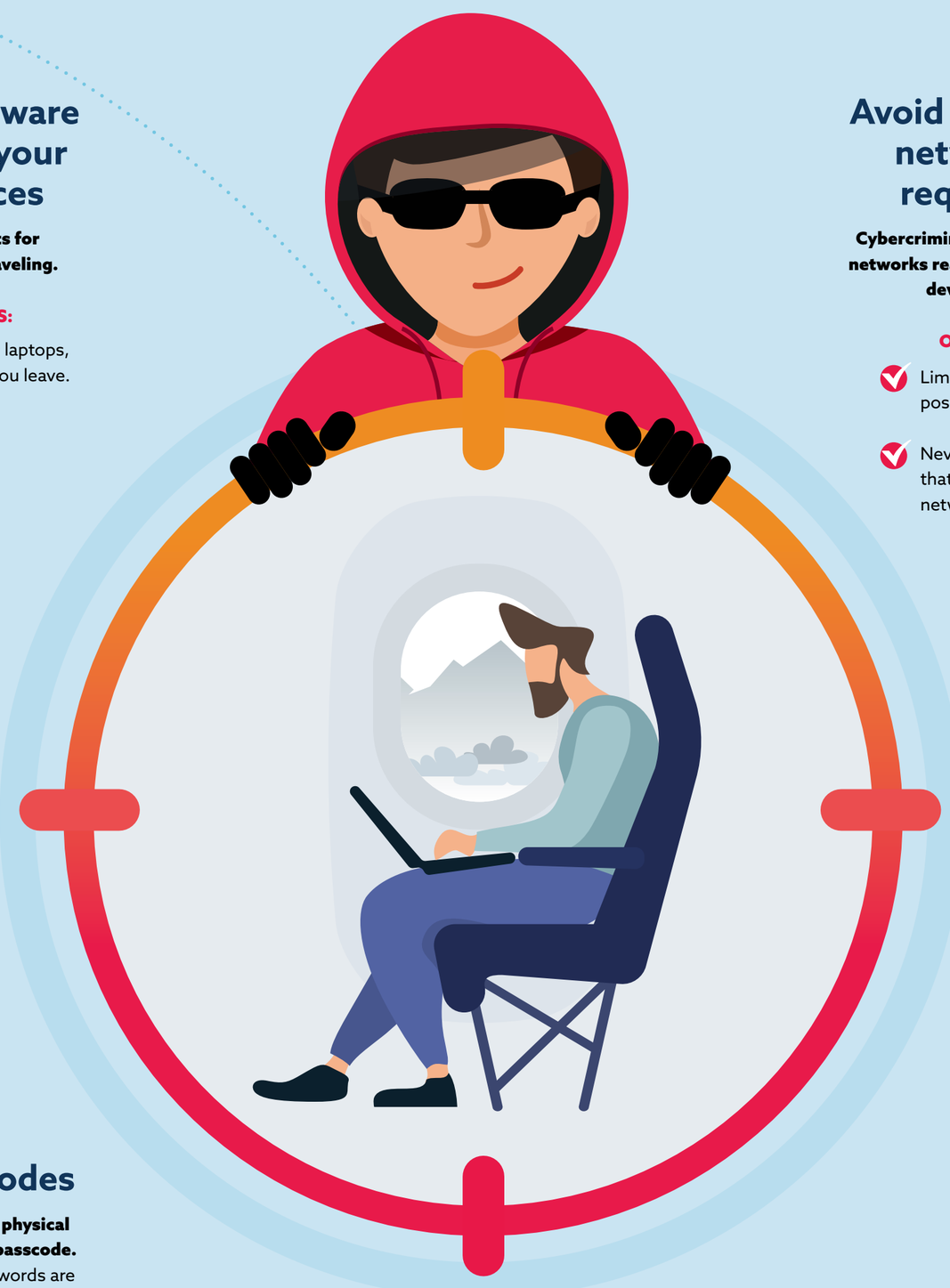
CYBER SAFETY DURING TRAVEL

NH PUBLIC WORKERS ARE AT RISK ON-THE-GO.

Whether by train, plane, or car — NH workers are often the targets of cybercrime on the go. Let's work together to bring the fun back to our domestic and overseas destinations by taking these important steps to protect data, devices, finances, and ourselves during travel — whether it's on another continent or even just a state or two away!

6 Easy Ways to Protect Yourself and NH



Make sure all software is up-to-date on your electronic devices

Devices are the easiest targets for cybercriminals while you are traveling.

OUR RECOMMENDATIONS:

- Perform all software updates on laptops, cellphones, and tablets before you leave.
- If a device is too old to update, consider leaving it at home to avoid the risk of compromise.

Avoid connecting to WiFi networks that don't require a password

Cybercriminals lurk on insecure and public WiFi networks ready to steal data, connect to insecure devices, or track your location.

OUR RECOMMENDATIONS:

- Limit the use of "Free WiFi" whenever possible, even in your home town.
- Never connect a computer or cellphone that has sensitive data to these types of networks without using a VPN.

Don't access sensitive personal information on apps or websites

When traveling, it is risky to access sensitive personal information, like banking information, financial applications, work email accounts, or websites and mobile apps containing access to data you'd like to protect. When possible, wait until you are home on your secure networks before accessing these types of sites.

Don't use debit cards

Financial frauds often occur during traveling. If you use a debit card and your card number is stolen through an insecure terminal or careless vendor, a criminal can drain your account while you are away. While you may not be responsible for lost funds, it will be a major inconvenience for you.

OUR RECOMMENDATIONS:

- Consider using a credit card to limit the impact a theft will have on your ability to pay your bills in the short term.
- Use debit cards only when absolutely required for day to day expenses.

Use strong passcodes

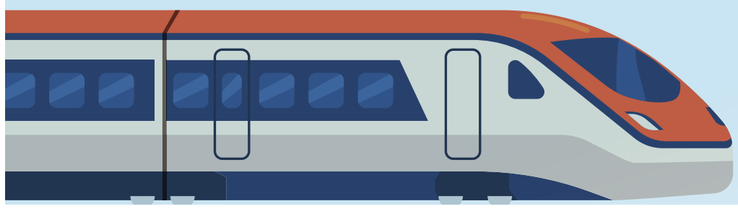
The second line of defense, after physical protection, is the use of a strong passcode. 4 digit pins and easy to guess passwords are an invitation for cyber crime while traveling.

OUR RECOMMENDATIONS:

- Use no less than 12 digit passcodes (remember spaces are acceptable or you can use a sentence!)
- Use no less than 6 digit pin numbers.
- When possible, use biometrics such as facial recognition or fingerprint protections.

Guard your devices and don't leave them unattended

Physical theft and unattended access to cellphones, computers, and tablets is still a major security issue in hotels, on public transportation, and in airports. Do not leave devices unattended, especially in hotel rooms when you leave for the day.



NH CYBER DEFENSE PROGRAM — POWERED BY ATOM

Primex³ NH Public Risk Management Exchange

New Hampshire DoIT

The Municipal Cyber Defense Grant is a collaboration between The ATOM Group, LLC. and the The New Hampshire Department of Information Technology. It is managed in coordination with the New Hampshire Public Risk Management Exchange and serves all New Hampshire based municipal governments, schools, and public sector organizations. For more information about the MCDG Program and the free services we provide, please visit us at https://www.theatomgroup.com/mcdp