



STAY SAFE

ONLINE



WATCH OUT FOR RED FLAGS

- An urgent request for payment via wire transfer or gift card is likely a scam.
- Do not engage with the requester.



KEEP DEVICES UPDATED

- Protect your computer, tablet, and phone from malicious software by keeping software current.
- Devices can be setup to automatically update or notify you when an update is ready to be installed.



KEEP BROWSERS UPDATED

- Make sure your web browser is current and you are using the privacy and security features.
- Like devices, web browsers can be setup to automatically update or notify you when an update is ready to be installed.



USE LONG, UNIQUE PASSWORDS

- Protect sensitive information with strong passwords (12+ characters) and keep them secret.
- Keep a record of your passwords away from your computer.



BE CAREFUL WITH LINKS IN MESSAGES

- Do not click on links, download attachments, or respond to messages that create a sense of urgency, like a problem with your bank account or taxes.
- To verify authenticity, use other known methods (like phone numbers or secure websites used previously).



KEEP PRIVATE INFORMATION PRIVATE

- The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data or commit other crimes.
- Assume any information you post online is visible to everyone.



SHOP CAREFULLY

- Use reputable websites.
- Look for assurances on the website that payment information will be secured.
- Never conduct financial transactions on a public computer.



PEOPLE ONLINE MAY BE FAKE

- Be wary of people appearing to be your friends or loved ones online.
- Criminals can easily hide their identity and appear trustworthy.
- If someone asks for money or sensitive information, it's likely a scam or fraud.



**HIGH
SPEED NV**



Nevada Governor's
Office of Science,
Innovation and
Technology