

February 2026

NNPS CYBERTIMES

THE LATEST UPDATES IN INFORMATION SECURITY

February: Awareness, Verification, & Smart Decisions

February marks the Lunar New Year, a time traditionally associated with renewal, awareness, and deliberate action. In the Year of the Fire Horse, the focus is often on energy, decisiveness, and staying alert, qualities that are equally important when navigating today's digital world.

As we continue building on January's focus on account security, this month shifts attention to how we interact with messages, requests, and other online communications. Cybercriminals rely heavily on trust, urgency, and familiarity to convince people to act quickly. February is about slowing that process down and making space for verification before responding

This Month's Cyber Focus: Verifying Messages Before Acting

Most cyber incidents do not begin with complex technology. They begin with a message—an email, a text, or a notification—that appears to come from someone you trust.

Attackers commonly impersonate:

- School staff or administrators
- Delivery services and online retailers
- Financial institutions or account providers
- Organizations offering assistance, updates, or support

These messages are often written to sound professional and helpful. The goal is not to look suspicious, but to appear familiar enough that verification feels unnecessary.



Common Red Flags to Watch For

Be cautious of messages that:

- Create urgency or pressure ("Act now," "Immediate response required")
- Ask you to bypass normal procedures or expectations
- Request information that would not typically be shared by email or text
- Contain links or attachments you were not expecting
- Ask you to keep the request confidential or act quickly

Even when a message looks official, discomfort or uncertainty is a sign to pause.

Cybercriminals depend on speed; safety improves when we slow down.



February 2026

NNPS CYBERTIMES

THE LATEST UPDATES IN INFORMATION SECURITY

Practical Habits That Help For Families

Families play an important role in helping students learn how to respond to messages, requests, and online communication safely. Students often move quickly between school platforms, personal email, messaging apps, and online services, and not every message they receive is trustworthy, even when it looks official or urgent.

Talking with students about verification and slowing down helps reduce risk both at home and at school. Many scams rely on creating pressure or excitement to trigger quick decisions. Helping students understand that it is okay to pause, question a message, and ask for help builds confidence and awareness rather than fear.

Helpful reminders for families include:

- Legitimate organizations do not pressure people to act immediately without allowing time to verify
- Personal information, passwords, and verification codes should never be shared through unexpected messages
- When something feels confusing, urgent, or unusual, stopping and asking a trusted adult is the right response

These conversations help students develop judgment and decision-making skills they will use throughout their academic and digital lives.



Final Thoughts

Cybersecurity is built one habit at a time. January focused on securing accounts; February focused on strengthening awareness, trust, and verification. Each month adds another layer of protection for students, staff, and families.

Thank you for staying alert, asking questions, and taking the time to slow down when something feels off. These thoughtful choices help keep our entire school division safer.

Need help or have questions? Our Technology team is always here to support you.

<https://sbo.nn.k12.va.us/technology/>

help.desk@nn.k12.va.us

(757) 881-5461 x.12411

Stay smart. Stay secure. Stay connected.

-Team InfoSec

