

September 2026

NNPS DIGITAL LEADERSHIP INITIATIVE

A CYBERSECURITY AWARENESS & PROFESSIONAL DEVELOPMENT SERIES

Identity Is the New Perimeter

For many years, cybersecurity focused on protecting the network perimeter, firewalls, filters, and technologies designed to keep threats out. Today's digital environment has fundamentally changed.

Staff and students securely access learning platforms, cloud services, and district resources from multiple locations and devices. In this environment, protecting access has become just as important as protecting systems. Identity is now the new perimeter.

Every account represents trust. Protecting that trust is one of the most important responsibilities we share as educators and public servants. Every day, staff and students access the digital resources that support teaching, learning, communication, and collaboration. Each successful login represents more than access to technology; it represents trust. Protecting our digital identities helps ensure that trust remains secure, allowing our schools to operate safely and confidently in an increasingly connected world.

This Month's Cyber Focus:

When an unauthorized individual gains access to an account, they often do not need to bypass sophisticated security controls; they simply sign in. Strong identity practices help ensure that only authorized users have access to district resources.

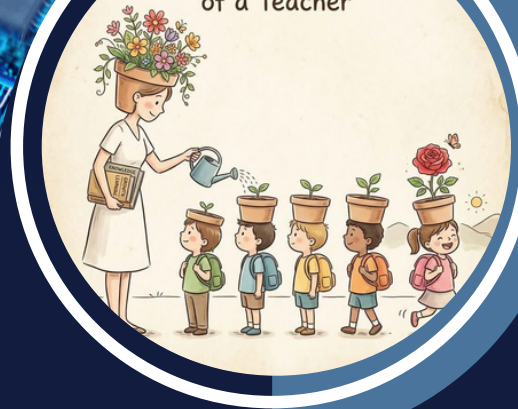
Good identity protection includes:

- Creating strong, unique passwords.
- Using Multi-Factor Authentication (MFA) whenever available.
- Keeping credentials private.
- Verifying unexpected login requests.
- Reporting suspicious account activity promptly.

Identity security is not about making access more difficult.

It is about making trust more reliable.

The Invisible Work of a Teacher



Common Warning Signs

Many account compromises begin with familiar situations, including:

- Unexpected requests to verify your account.
- Emails directing you to unfamiliar login pages.
- Requests for verification codes.
- Password reset notifications you did not initiate.
- Messages creating unnecessary urgency.

If something seems unusual, pause and verify before taking action.

Security Spotlight

Trust Begins with Identity

Every time you sign in, your identity tells a system who you are and what information you are authorized to access.

Protecting that identity protects more than your account, it helps safeguard student information, district resources, and the trust placed in each of us.

Identity security is no longer just a technical control. It is a professional responsibility.

Just as we safeguard classrooms, student records, and physical resources, we also have a responsibility to protect the digital identities that provide access to them. Every secure login contributes to a safer and more resilient learning environment.



September 2026

NNPS DIGITAL LEADERSHIP INITIATIVE

A CYBERSECURITY AWARENESS &
PROFESSIONAL DEVELOPMENT SERIES

Smart Habits That Help

Strong identity protection begins with consistent habits:

- Use unique passwords for every account.
- Never share passwords or MFA verification codes.
- Access important accounts through trusted websites or applications.
- Protect login information from being visible to others.
- Report unusual account activity promptly.

Small habits practiced consistently provide strong protection over time. In cybersecurity, identity is often the first line of defense—and increasingly, the last. Protecting your credentials protects not only your information, but the people, systems, and community that depend on them.

For Families

Families play an important role in helping students build lifelong digital habits. Encouraging good cybersecurity practices at home reinforces what students learn at school and helps them become responsible digital citizens.

Talk with your child about the importance of protecting their online identity and encourage them to:

- Create strong, unique passwords for important accounts.
- Keep login credentials private, even from friends.
- Understand why verification codes should never be shared with anyone.
- Recognize suspicious login requests, unexpected text messages, or fake websites designed to steal personal information.
- Enable multi-factor authentication (MFA) whenever it is available for personal accounts.

A simple conversation today can help prevent account compromises tomorrow. As students grow and begin using more online services for school, work, banking, and everyday life, understanding how to protect their digital identity becomes an essential life skill. Helping them build those habits now prepares them to navigate tomorrow's digital world with confidence.



Final Thoughts

Technology will continue to evolve. The importance of protecting identity will not.

Every secure login, every thoughtful password, and every verification step strengthens the trust that allows our schools to teach, learn, and collaborate safely.

Strong identities create strong organizations. And strong organizations are built one secure decision at a time. Because in the end, cybersecurity isn't just about protecting systems; it's about protecting the people who rely on them every day.

Until next time,
-Office of Information Security

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

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

tsc@nn.k12.va.us

(757) 881-5461 x.12411

