October 2026

NNPS DIGITAL LEADERSHIP INITIATIVE

A Cybersecurity Awareness & Professional Development Series



Social Engineering in the AI Era

Artificial Intelligence has changed how we work, communicate, and learn. It has also changed how cybercriminals attempt to deceive us.

AI can create remarkably convincing emails, text messages, images, videos, and even voices. Yet while today's attacks may look and sound more believable, the objective hasn't changed.

Social engineering still relies on familiar human tendencies - trust, curiosity, urgency, and the desire to help.

This Month's Cyber Focus:

Technology Changes. The art of manipulation doesn't.

Social engineering isn't primarily about defeating technology. It's about influencing people into making a decision that benefits an attacker.

Imagine receiving an urgent message that appears to come from a supervisor asking you to send information, open a document, or complete an unusual task. The name looks right. The message sounds convincing. A voice message may even sound like the person you know.

As digital content becomes easier to imitate, verification becomes more important than appearance.

Common Warning Signs

Be cautious when a message:

- **Creates unusual or unnecessary urgency.**
- **Requests confidential information unexpectedly.**
- **Discourages you from verifying the request.**
- **Uses emotion or authority to pressure you.**
- **Asks you to bypass normal procedures.**

In an AI-enabled world, credibility and authenticity are not always the same thing. Something can look, sound, and feel convincing without being genuine.

Security Spotlight

Critical Thinking Is a Security Skill

AI can generate convincing content. It cannot make a fraudulent request legitimate.

Before responding to something unexpected, ask:

- Does this fit our normal procedures?
- Can I independently verify who is asking?
- Why does this need to happen immediately?

Those few seconds of critical thinking can interrupt an attack before technology ever needs to.

October 2026

NNPS DIGITAL LEADERSHIP INITIATIVE

A Cybersecurity Awareness & Professional Development Series



Smart Habits That Help

Build verification into your normal routine:

- **Confirm unusual requests through a separate, trusted communication method.**
- **Verify identities before sharing sensitive information.**
- **Don't rely solely on caller ID, display names, images, or online profiles.**
- **Report suspicious communications promptly.**
- **Treat unexpected urgency as a reason to verify, not a reason to hurry.**

Every member of our school community contributes to the security of our information and systems we share.

For Families

The same principles apply at home.

Encourage students to question unexpected messages, verify unusual requests with a trusted adult, and remember that voices, images, videos, and online identities can now be artificially generated or altered.

Digital literacy increasingly means knowing not only how to find information, but how to evaluate whether that information deserves our trust.

Rather than teaching students to distrust everything online, we can teach something more useful:

Trust thoughtfully. Verify when it matters.

Final Thoughts

Artificial Intelligence will continue to evolve, and the technology used to create convincing content will continue improving.

Our advantage doesn't require becoming an AI expert. It requires developing habits that technology cannot make obsolete: thinking critically, following established procedures, verifying unusual requests, and speaking up when something doesn't seem right.

Every thoughtful decision strengthens the security and digital resilience of our schools, families, and community.

Remember, critical thinking is one of the most valuable security tools we possess.

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