NEW YORK STATE REGIONAL INFORMATION CENTERS

# DATA PRIVACY AND SECURITY

*Educational agencies are facing an increasing number of cyberattacks, leading to data theft, ransomware incidents that lock down critical systems, and service disruptions. Strengthen your district's security posture with these simple tips.*

## DATA PROTECTION REMINDERS

| | | |
|---|---|---|
| **E-MAIL BEST PRACTICES** |  | Verify the context of unexpected messages, carefully inspect email addresses and links before clicking, and avoid replying to or sending sensitive information through email if the message seems suspicious. |
| **PASSWORDS** |  | Use strong, unique passwords with a mix of characters, avoid personal details like birthdays or names, consider using a password manager, and never share your passwords with anyone. |
| **MULTI-FACTOR AUTHENTICATION** |  | Multi-factor authentication (MFA) adds an extra layer of security by requiring a second verification step, like a code or app, and enabling it in schools helps strengthen the protection of sensitive systems. |
| **DATA HANDLING** |  | Always protect personally identifiable information (PII) by sharing it only with approved users through secure platforms, and consult district leadership before entering PII into any system. |
| **PORTABLE DEVICES** |  | Keep portable devices secure by storing them in a safe place when not in use, protecting them with a strong password and encryption, and avoiding public Wi-Fi connections to safeguard data. |
| **ARTIFICIAL INTELLIGENCE** |  | Use AI tools appropriately by understanding their purpose, being mindful of potential biases, avoiding PII without district approval, and recognizing AI's evolving capabilities and future potential. |

***Human behavior is at the root of 95% of all cyber security incidents.***

*For additional resources on data privacy and security practices, visit www.ricone.org or contact your local Regional Information Center.*

**VIDEO LINK**
https://youtu.be/sSaAoepmLLs



*Updated: October 12, 2024*