HMIS Newsletter

Cyber Security Edition

Homeless Alliance of WNY• March 2021

Cyber Security 101

Cyber Security Basics

- You are the first line of defense! The first step to reducing security risks is to be aware of scams and what they look like.
- Follow your agency's IT policies and procedures and if you are unsure of something ask them! They will be more than happy (hopefully) to answer your questions or concerns because...
- Prevention is better than reacting. It's easier to stop any attack before they happen than to deal with the fallout.
- Use stranger danger tactics. If you don't know who is sending an email or request its ok to be suspicious.
- Be wary of social engineering which is a manipulation technique to get your information.
- Take basic precautions such as using strong passwords, not clicking weird links or websites, and not downloading data on unsecure platforms.

Common Scams: Phishing and Ransomware

- "**Phishing**" is one of the most common type of cyber attacks. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details.
- **Ransomware** is the term used when unauthorized parties extort money from organizations. Ransomware is a type of malicious software that takes over your computer and prevents you from accessing files until you pay a ransom.

Things to look out for:

- Weird grammar
  - Misspellings, odd sentence structure, or weird requests are common giveaways of phishing scams.
- The actual email address
  - Checking the sender's actual email address is a good method of determining if the email is legitimate.
- Suspicious links or attachments
  - Never click on weird links or open attachments from these emails! Think before you click!

HMIS Security

HAWNY takes the security of HMIS seriously. All users are expected to follow the guidelines set forth by the user agreement and use basic security methods to protect their client's data. If you notice any threats or risks please notify HAWNY staff ASAP.

If any user violates HMIS security/privacy policies the incident will be recorded, the user will be be given a one time warning, and required to sit through a mandatory security course. A second violation will result in HMIS user account termination.

Steps To Take

- Change passwords when prompted.
- Don't save HMIS passwords on computers.
- Never share passwords or usernames.
- Use strong passwords!
    - 8 characters long with a mix of numbers, letters, and cases.
- Don't login from public wifi or networks
- Use common sense. If something seems weird double check or report it!
- Don't send emails with Personal Identifying Information.
- Follow your own agency's IT procedures.
- Notify HAWNY of staff turnover for user account management