WHO are we empathizing with?

A user who understands the importance of cybersecurity but may not be technically proficient.

What do they HEAR?

Security alarms and triggers due to suspicious activities.
Discussions about latest threat intelligences.
Colleagues and members discussing recent security threats.

What do they SAY?

"I'm worried about the security of my computer."

"I'm not sure if my antivirus software is reliable enough."

"I need something that can protect my personal information."

"I don't want to lose important data to malware."

MALWARE DETECTION AND CLASSIFICATION

What do they THINK?

"I don't want to be the victim of a cyber-attack."

"Is there a way to be more proactive about my computer's security?"

"I need a solution that doesn't slow down my computer."

"I wish there was a tool that could detect new types of malware."

PAINS

- Fear of losing personal data or sensitive information.
- Frustration with existing antivirus software's limitations.
- Uncertainty about which websites or files are safe.
- Desire for a solution that works in the background without disrupting regular computer use.

GAINS

- Peace of mind knowing their computer is secure.
- Confidence in the effectiveness of the malware detection tool.
- Time saved by not having to manually check for malware.
- A sense of control over their digital security.

What do they DO?

Regularly checks for software updates and security patches.

Runs periodic malware scans using antivirus software.

Avoids suspicious websites and emails.

Backs up important files to an external drive or cloud storage.

What do they FEEL?

Concerned about the increasing sophistication of malware.

Frustrated with false alarms from antivirus programs.

Anxious about potential data breaches and identity theft.

Hopeful for a more robust and reliable malware detection solution.