RISKY BUSINESS
Protecting Survivors from Cybersecurity Threat

Ashley Schwedt
Director of Campus Relationships

Eliza Milliken
Community Liaison
THREAT MODELING

A threat model is a way to determine the security of a system or process by identifying threats and vulnerabilities.

It is most often used with software and applications to create more efficient and safe systems and processes.

Like everything, its translatable!
THREAT MODELING

• What information do I have?
• How is that information stored/shared?
• Who wants that information?
• How might they get it?
• How can I prevent them getting it?
THREAT MODELING

flow of information

- survivor's story
  - professor, advisor, campus police, etc.
  - friend, family, roommate, etc.
- Title IX coordinator
  - Title IX investigators
  - support folks (counseling, dean, etc.)
  - perpetrator
  - witnesses
  - survivor
  - survivor's friends

@callisto
@ashSchwedt
@eliza_milliken
THREAT MODELING
flow of information

survivor's story

you
THREAT MODELING
storing & sharing of information

- in their brain
- in a notebook
- in-person
- email
- form submission
- on their phone
- friend, family, roommate, etc.
- on their computer
- in-person, phone call, email
- Title IX coordinator
- email, printed papers
- on their computer
- email, phone call, in-person
- on their computer, in a file cabinet
- email, phone call
- perpetrator
- witnesses
- survivor
- survivor's friends
- support folks (counseling, dean, etc.)
- on their computer, in a file cabinet
- email, phone call
- on their computer, in a file cabinet
- email, phone call
THREAT MODELING
identifying the information

What is this information?

- Survivor’s name & contact
- Perpetrator’s name & contact
- Description of the incident
- Names of witnesses/bystanders
- That a report was made & when
- When the incident happened
- Where the incident happened
THREAT MODELING
who wants the information

Who wants it?

- Perpetrator
- Opportunist/Gossip
- Lawyers
- Parents
- Hackers
- Other?

survivor’s story

- Survivor’s name & contact
- Perpetrator’s name & contact
- Description of the incident
- Names of witnesses/bystanders
- That a report was made & when
- When the incident happened
- Where the incident happened
THREAT MODELING
who wants the information

survivor's story
- in their brain
- in a journal
- on their phone
- phone call or text, other messaging tool

OPPORTUNIST
- in a notebook
- professor, advisor, campus police, etc.
- email
- form submission
- in-person

GOSSIP
- in-person
- email

PERPETRATOR
- in-person, phone call, email
- email, printed papers
- email, phone call

LAWYER
- email, phone call
- email, phone call

HACKER
- on their computer
- email, phone call, in-person
- on their computer, in a file cabinet

support folks (counseling, dean, etc.)
- email, phone call
- email, phone call
- on their computer, in a file cabinet

PARENT
- email, phone call
- email, phone call

survivor's friends
- email, phone call

Title IX investigators
- email, phone call
- email, phone call
THREAT MODELING
why is this scary

DIGITAL

1. Email is insecure
   • Would you send the password to your bank account on a piece of paper to your friend? If you did, would you cover it with a thicker piece of paper, fold over the paper, send it certified requiring a signature, etc.?

2. Human error is the #1 cause for data breach
   • Are you about to identify a phishing email? What if you got an email that looked like it was from Advocate asking you to re-enter information because it didn’t save correctly?
THREAT MODELING
why is this scary

PHYSICAL

1. Printers
   • When you send something to a printer, can you guarantee that you’re the one to get it? Does it get stored in a printing queue at any point?

2. Screensharing
   • Do you share your screen with anyone? Do you share your whole screen or just your application window? Are people able to see your emails?

3. Security of your machine
   • Can anyone see your screen when they walk by? Do you logout whenever you leave? What does IT recommend?
THREAT MODELING
protecting the information

Protect the survivor

- Encrypt your emails
- Be careful with printing
- Don’t fall for phishing
- Create policies, practices, and procedures
- Tint your computer screen
- Never share your full screen
- What else?!
How can you translate this to advising survivors how to protect themselves?

<table>
<thead>
<tr>
<th>WHAT INFO?</th>
<th>SHARED/STORED?</th>
<th>WHO WANTS IT?</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Current location</td>
<td>- Social media</td>
<td>- Perpetrator</td>
</tr>
<tr>
<td>- Friends/roommates</td>
<td>- School directory</td>
<td>- Perpetrator's friends</td>
</tr>
<tr>
<td>- Class schedule</td>
<td>- In-person conversation</td>
<td>- Lawyers</td>
</tr>
<tr>
<td>- Address</td>
<td>- Journal/notebook</td>
<td>- Family</td>
</tr>
<tr>
<td>- Alcohol use</td>
<td>- Computer</td>
<td>- Gossips/Opportunists</td>
</tr>
<tr>
<td>- Their story</td>
<td>- Browser tracking</td>
<td>- Other?</td>
</tr>
</tbody>
</table>

@callisto
@ashSchwedt
@eliza_milliken