Allegro - Worksheet 10	Information Asset Risk Worksheet			
Information Asset Risk	**Threat**	Information Asset	Personal Accounts credentials	
		Area of Concern	Http traffic eavesdropping	
		(1) Actor *Who would exploit the area of concern or threat?*	Threat actor with access to home network	
		(2) Means *How would the actor do it? What would they do?*	Many smartdevice have a web interface for configuration, which is often served in plain HTTP. An attacker can sniff this traffic and easily retrieve login credentials.	
		(3) Motive *What is the actor's reason for doing it?*	Successful eavesdropping gives the attacker access to the device. The same credentials can be tested to control other devices in the network. The hacked device can serve as a starting point for other malicious activities.	
		(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☐ **Destruction** ☑ **Modification** ☐ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality and Integrity of credentials breached	
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☐ **Medium** ☑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Compromise of the device	Reputation & Confidence	H	12
	Financial	L	5
If the same password was reused, the attacker can gain access to multiple devices at the same time.	Productivity	H	9
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
		Relative Risk Score	**39**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	☑ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
IoT devices	If the device provides this possibility, enable HTTPS access to configuration page
Passwords	Use a password manager to generate random and unique passwords for devices.
Network	Monitor new devices accessing the home network and verify their identity.

Allegro - Worksheet 10	Information Asset Risk Worksheet			
Information Asset Risk	**Threat**	Information Asset	Personal Accounts credentials	
		Area of Concern	Http traffic eavesdropping - residual risk	
		(1) Actor *Who would exploit the area of concern or threat?*	Threat actor with access to home network	
		(2) Means *How would the actor do it? What would they do?*	Many smartdevice have a web interface served in plain HTTP. An attacker can sniff this traffic and easily retrieve login credentials.	
		(3) Motive *What is the actor's reason for doing it?*	Successful eavesdropping gives the attacker access to the device. The same credentials can be tested to control other devices in the network. The hacked device can serve as a starting point for other malicious activities.	
		(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☐ **Destruction** ☑ **Modification** ☐ **Interruption**	
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality and Integrity of credentials breached	
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High**	☐ **Medium** ☑ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Compromise of the device	Reputation & Confidence	L	4
	Financial	L	5
	Productivity	L	3
	Safety & Health	L	6
	Fines & Legal Penalties	L	1
	User Defined Impact Area	L	2
		Relative Risk Score	**21**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☑ **Accept**	☐ **Defer**	☐ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*

Allegro - Worksheet 10	INFORMATION ASSET RISK WORKSHEET				
Information Asset Risk	**Threat**	Information Asset	Personal Accounts credentials		
		Area of Concern	Phishing emails		
		(1) Actor *Who would exploit the area of concern or threat?*	External threat actor		
		(2) Means *How would the actor do it? What would they do?*	Phishing emails may impersonate smart devices service providers and trick users into opening malicious links or give away their credentials.		
		(3) Motive *What is the actor's reason for doing it?*	Credentials allow access to smart home controls, and can be tested to login on other websites.		
		(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☐ **Destruction** ☑ **Modification** ☐ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality and Integrity of credentials breached		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	☑ **High**	☐ **Medium**	☐ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Compromise of the account	Reputation & Confidence	H	12
	Financial	L	5
If the same credentials were reused, the attacker can gain access to multiple services.	Productivity	M	6
	Safety & Health	M	12
	Fines & Legal Penalties	L	1
	User Defined Impact Area	H	6
	Relative Risk Score		**126**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☐ **Accept**	☐ **Defer**	☑ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Email clients	Use modern mail clients which provides antispam and antiphishing filters.
People	Raise awareness in household members about phishing and instruct them on verifying emails authenticity and domains of URLs.
Credentials	Use unique and random credentials. Provide every household member a specific account, which can be immediately shut down in case of compromise.
Smarthome	Monitor user activities and investigate suspect or unexpected behaviors.
Logins	Enable 2FA authentication when available, especially for accounts which can access the system from the internet.

Allegro - Worksheet 10	Information Asset Risk Worksheet

Information Asset Risk

Threat

Information Asset	Personal Accounts credentials
Area of Concern	Phishing emails - residual risk

(1) Actor *Who would exploit the area of concern or threat?*	External threat actor
(2) Means *How would the actor do it? What would they do?*	Phishing emails may impersonate smart devices service providers and trick users into opening malicious links or give away their credentials.
(3) Motive *What is the actor's reason for doing it?*	Credentials allow access to smart home controls, and can be tested to login on other websites.
(4) Outcome *What would be the resulting effect on the information asset?*	☑ **Disclosure** ☐ **Destruction** ☐ **Modification** ☑ **Interruption**
(5) Security Requirements *How would the information asset's security requirements be breached?*	Confidentiality and Integrity of credentials breached
(6) Probability *What is the likelihood that this threat scenario could occur?*	☐ **High** ☐ **Medium** ☑ **Low**

(7) Consequences

What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?

Compromise of the account, requiring the admin to reset its password.

(8) Severity

How severe are these consequences to the organization or asset owner by impact area?

Impact Area	Value	Score
Reputation & Confidence	L	4
Financial	L	5
Productivity	L	3
Safety & Health	L	6
Fines & Legal Penalties	L	1
User Defined Impact Area	L	2

Relative Risk Score **21**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

☑ **Accept**	☐ **Defer**	☐ **Mitigate**	☐ **Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
	t