# Santé publique pour la prévention des attaques par logiciels malveillants

Fanny Lalonde Lévesque
Étudiante au doctorat, Polytechnique Montréal
Chercheuse appliquée, Element AI

Journée de la recherche du FRQNT
16 mai 2018

# Computer threats

## What's the problem ?

**2.3** connected devices *per capita* in 2016 → **3.6** in 2021 [1]
**4.6** trillion of Internet users in 2021 [1]

**285,000** new malware samples everyday in 2017 [2]
**136** public data breaches in 2005 → **7,885** in 2018 [3]

Ransomware alone costed **5** billion USD in 2017 [4]
Global cost of attacks estimated at **6** trillion USD in 2021 [4]

[1] Cisco System, 2017. [2] PandaLabs, 2017. [3] Privacy Rights ClearingHouse, 2018. [4] Cybersecurity Ventures, 2017.

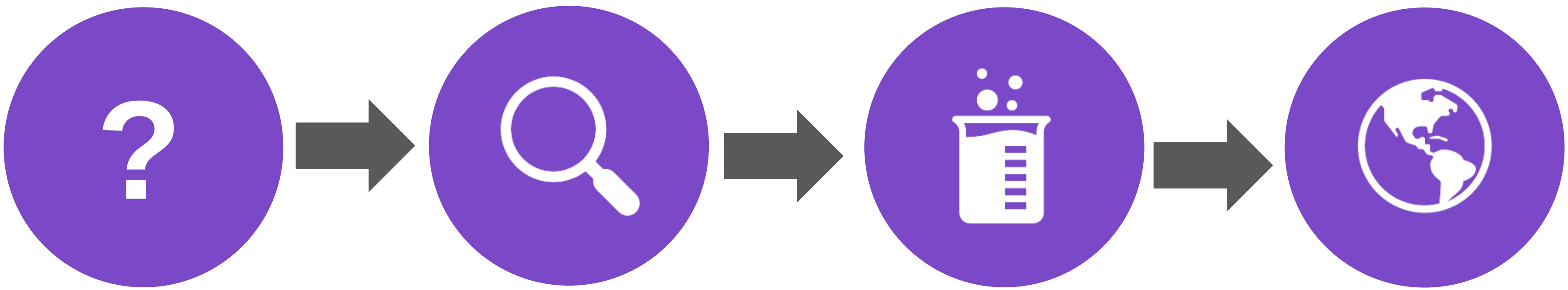
# Prevention

## What are the solutions ?

# Public health

> “Public health is defined as the science of protecting the safety and improving the health of communities through education, policy making and research for disease and injury prevention.”
>
> — Public Health Agency of Canada

# Public health framework



**Define the problem**

Identify and understand ‘who’, ‘what’, ‘when’, ‘where’, and ‘how’.

**Identify risk and protective factors**

Identify the causes and correlates related to the problem

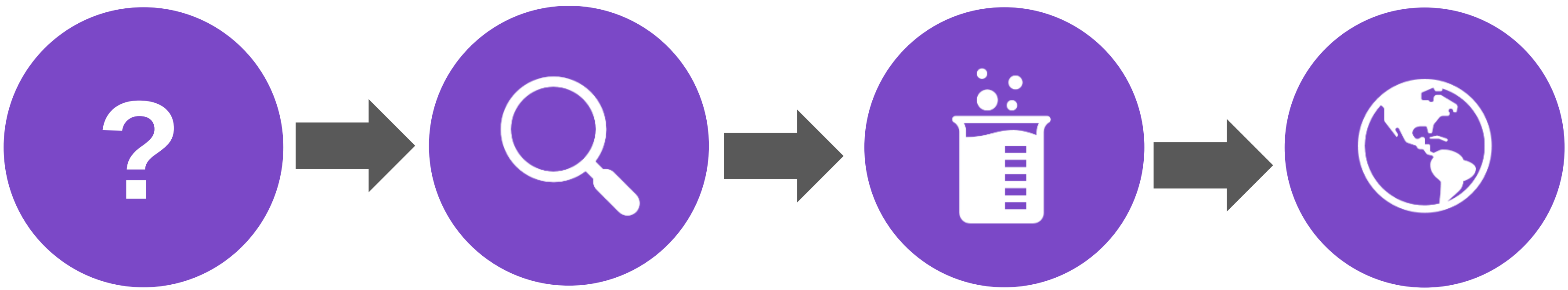
**Develop and test strategies**

Develop and evaluate prevention strategies

**Ensure global adoption**

Implement and disseminate the strategies

# Application to malware prevention



**Define the problem**

Study the trends and patterns of malware attacks

**Identify risk and protective factors**

Identify the causes and correlates related to Malware attacks

**Develop and test strategies**

Develop and evaluate strategies aimed at preventing and/or reducing malware attacks

**Ensure global adoption**

Implement and promote strategies proven effective at preventing and/or reducing malware attacks

# Application to malware prevention

**Define the problem**

Study the trends and patterns of malware attacks

**Identify risk and protective factors**

Identify the causes and correlates related to Malware attacks

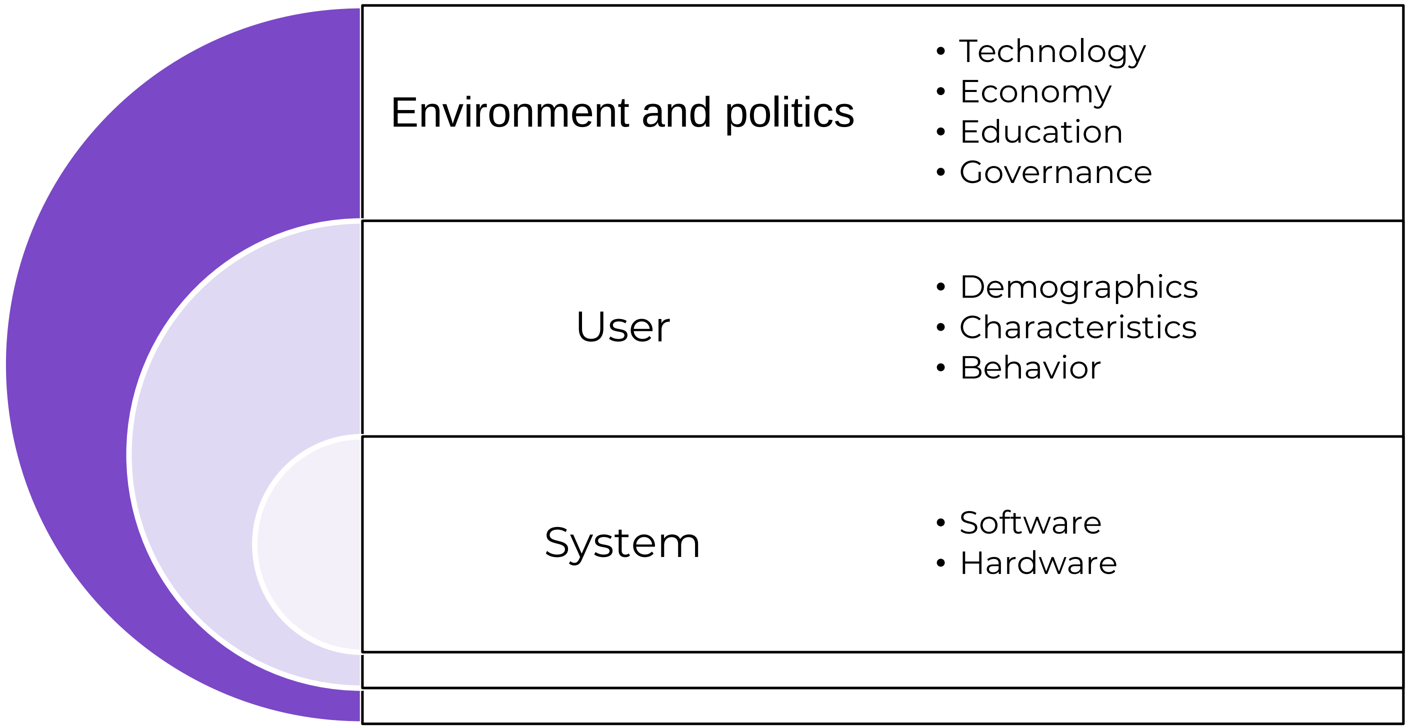
**Develop and test strategies**

Develop and evaluate strategies aimed at preventing and/or reducing malware attacks

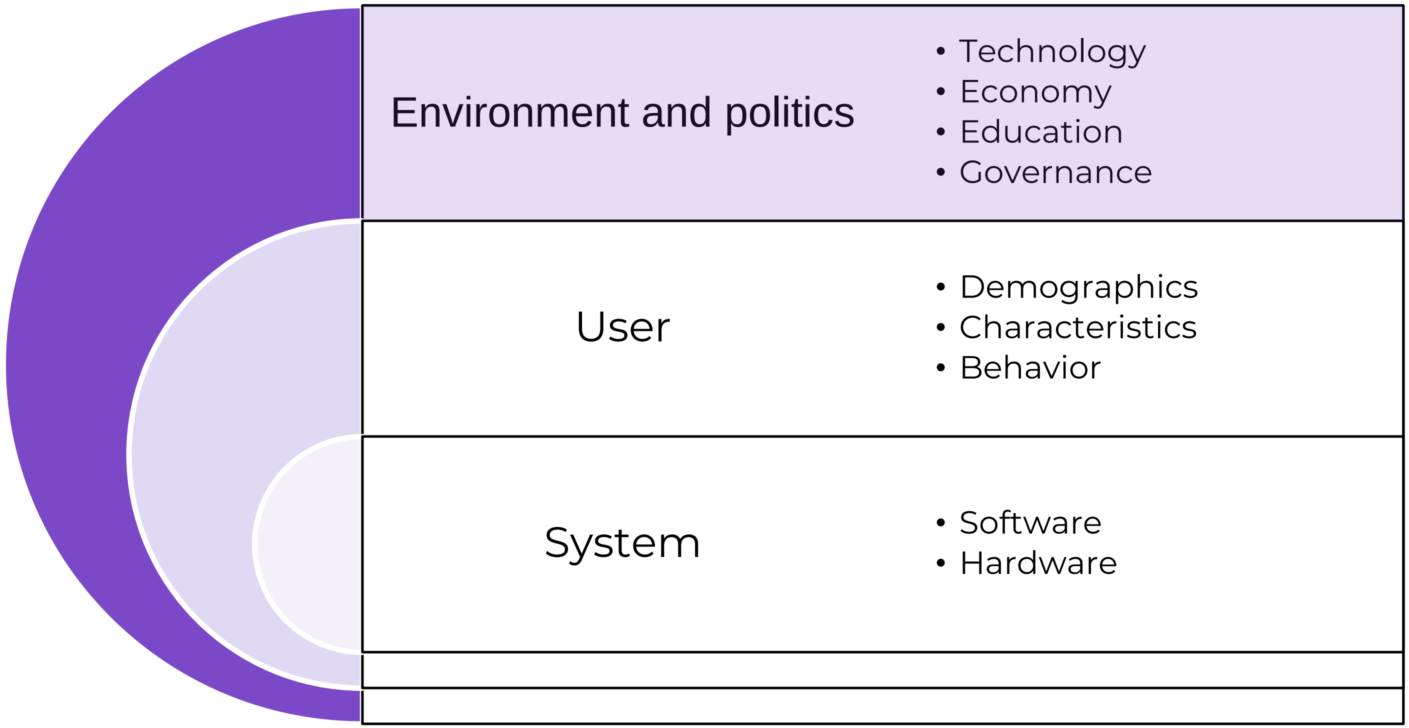
**Ensure global adoption**

Implement and promote strategies proven effective at preventing and/or reducing malware attacks

# Identify risk and protective factors



# Identify risk and protective factors



# National-level factors

What **national-level** factors correlate with the rate of malware infections ?

**10+ M**

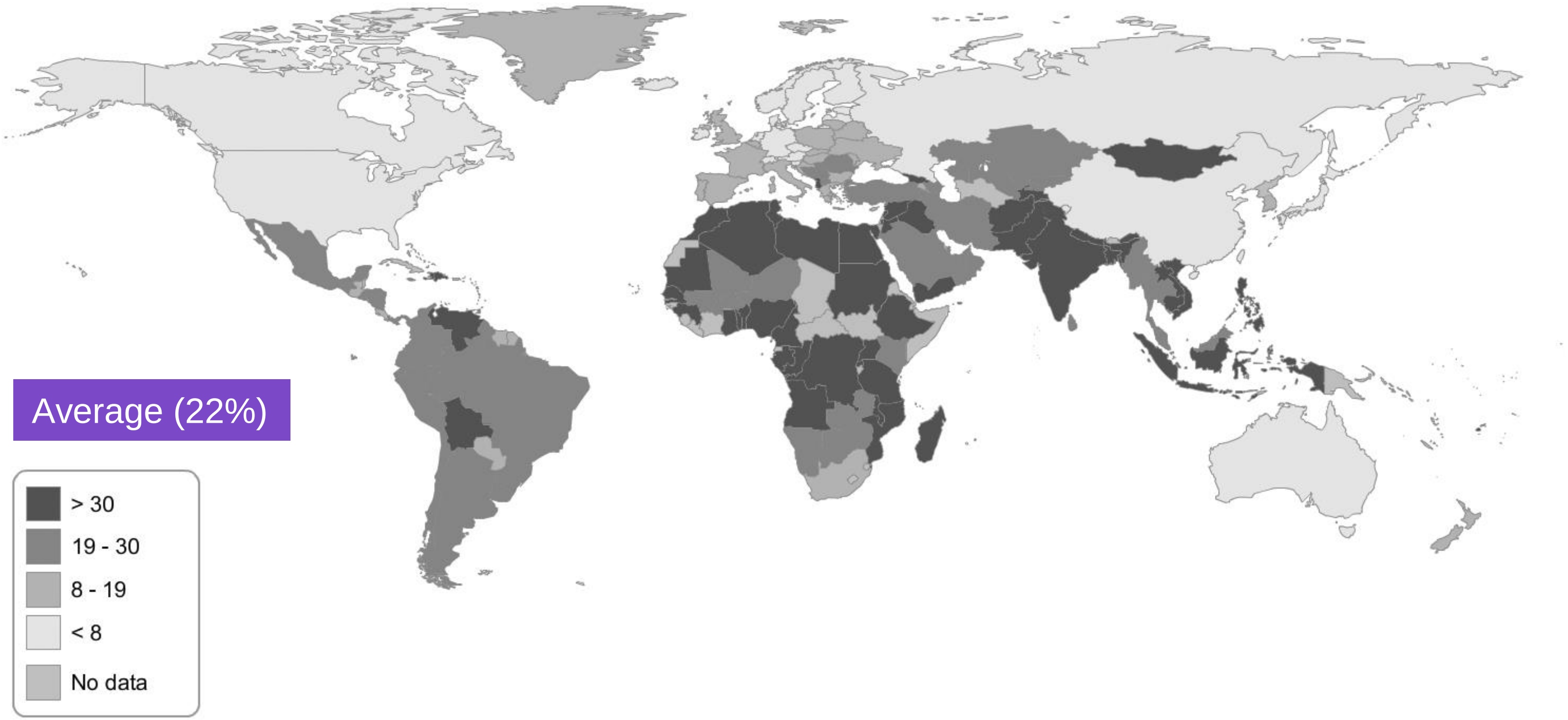
10+ million unprotected devices running Windows
Malware infections from MSRT
June to September 2014

186 countries
15 factors

Economy | Education | Technology | Cybersecurity

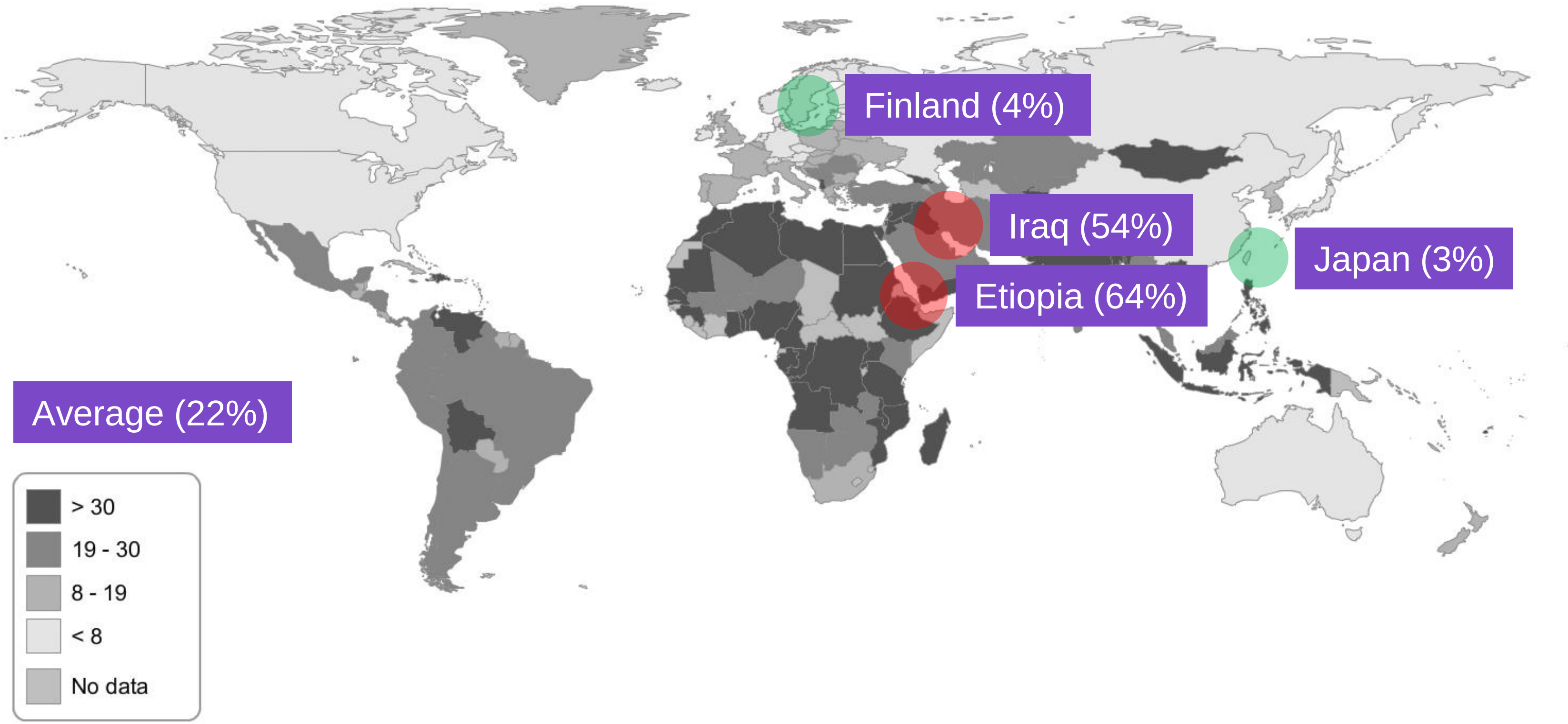
F. Lalonde Lévesque et al., *National-level risk assessment: A multi-country study of malware infections*, WEIS 2016.

# National-level factors




F. Lalonde Lévesque et al., *National-level risk assessment: A multi-country study of malware infections*, WEIS 2016.

# National-level factors




F. Lalonde Lévesque et al., *National-level risk assessment: A multi-country study of malware infections*, WEIS 2016.

# National-level factors

## Multi-level risk analysis by **HDI status**

**HDI**
>= 0.8

45 countries
10% average infection rate

**10%**

0.8 >
**HDI**
>= 0.55

74 countries
26% average infection rate

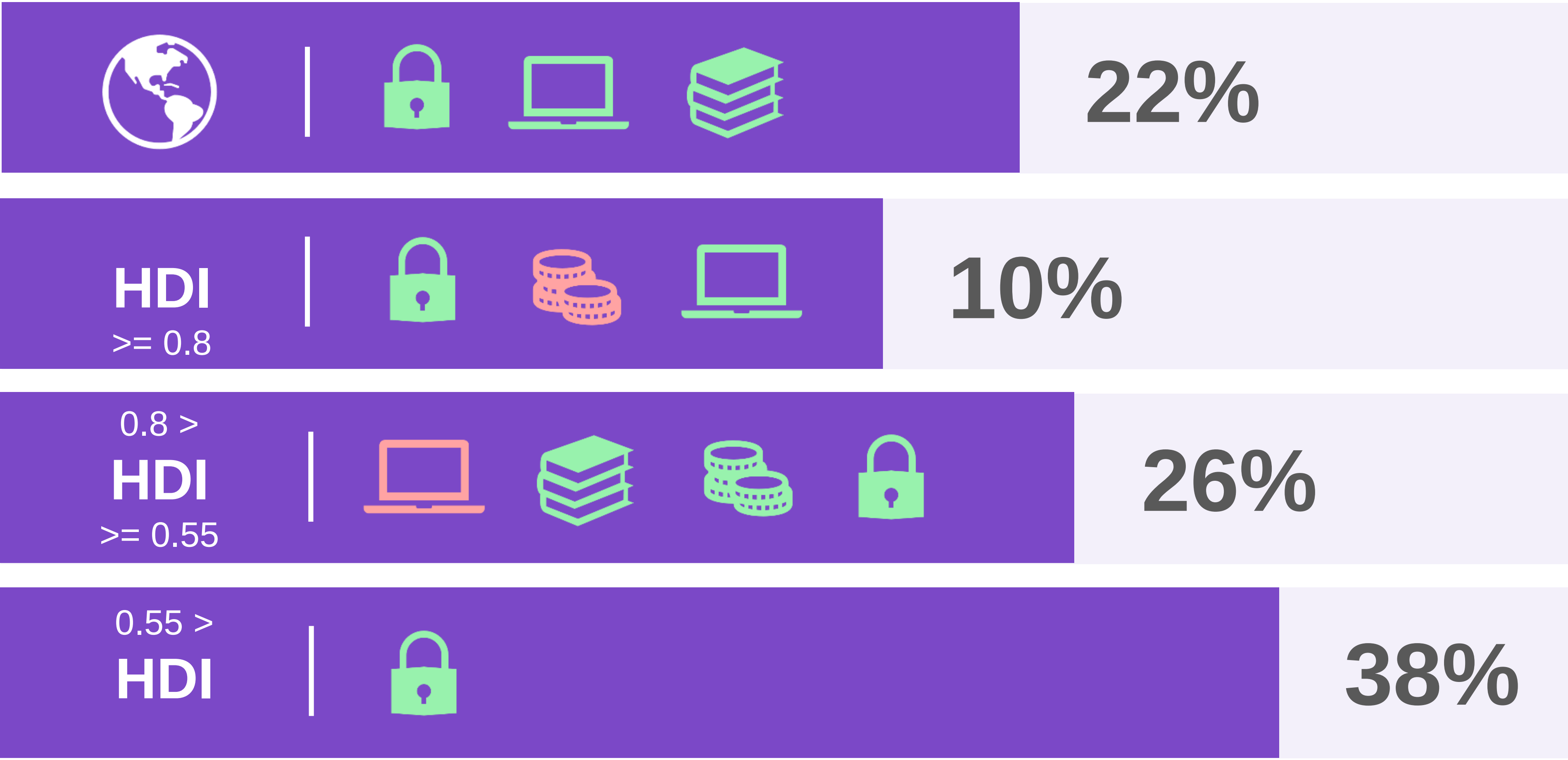
**26%**

0.55 >
**HDI**

26 countries
38% average infection rate

**38%**

F. Lalonde Lévesque et al., *National-level risk assessment: A multi-country study of malware infections*, WEIS 2016.




F. Lalonde Lévesque et al., *National-level risk assessment: A multi-country study of malware infections*, WEIS 2016.

# Identify risk and protective factors

| | |
|---|---|
| Environment and politics | • Technology<br>• Economy<br>• Education<br>• Governance |
| User | • Demographics<br>• Characteristics<br>• Behavior |
| System | • Software<br>• Hardware |

# User-level factors

Are **age** and **gender** independent risk factors of malware victimisation ?

**10+ M**

10+ million devices running Windows 10
Malware encounters from Windows Defender
October to December 2015

**Male**
Female

0-17, 18-24, 25-34, 35-49, **50+**

F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# User-level factors

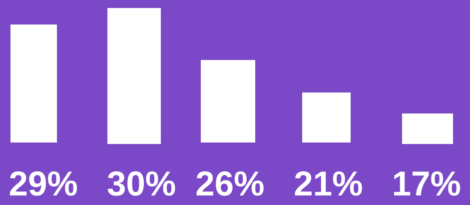
## Risk analysis of **age** and **gender**

**1.32**

Male are 1.32 more likely to encounter malware than female


**1.99**

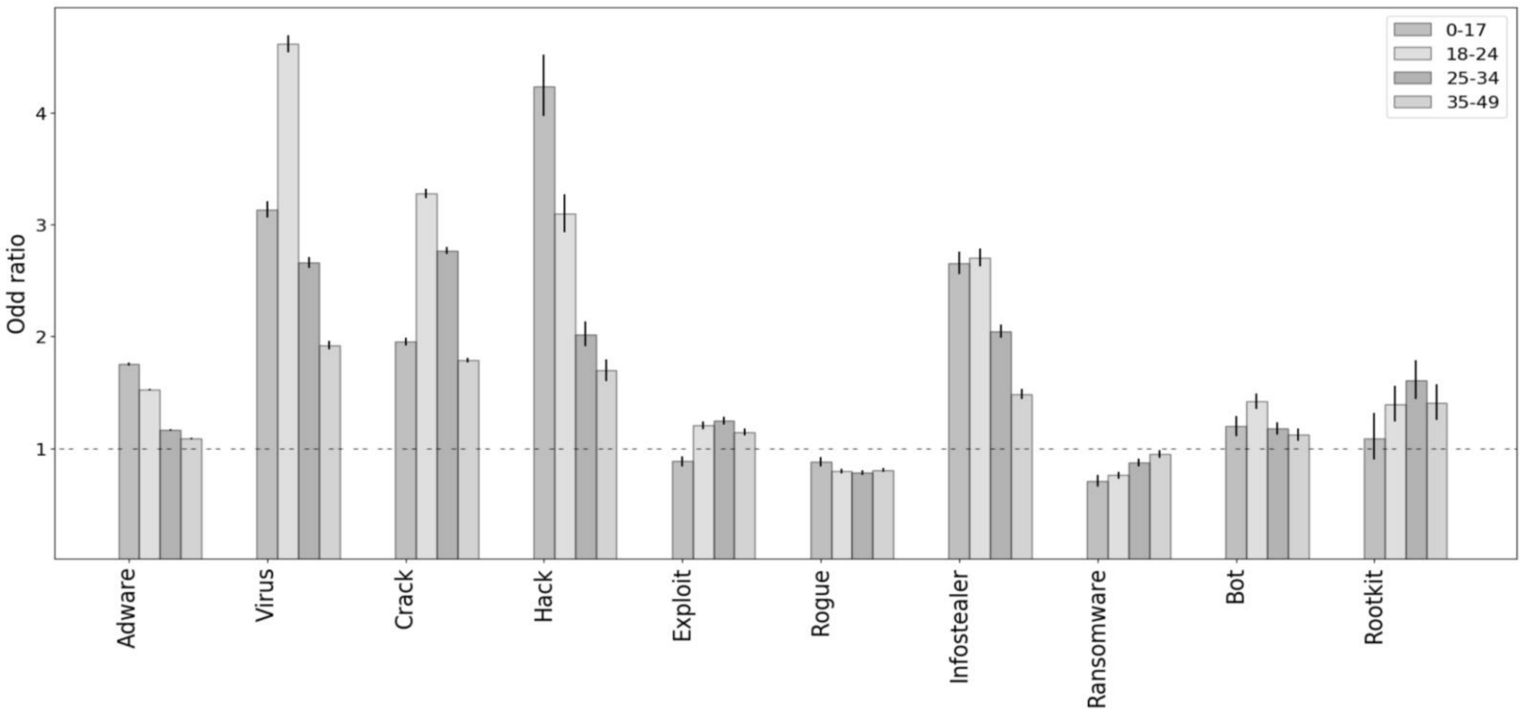
Age group 18-24 is 1.99 more likely to encounter malware than the 50+ age group




F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# User-level factors

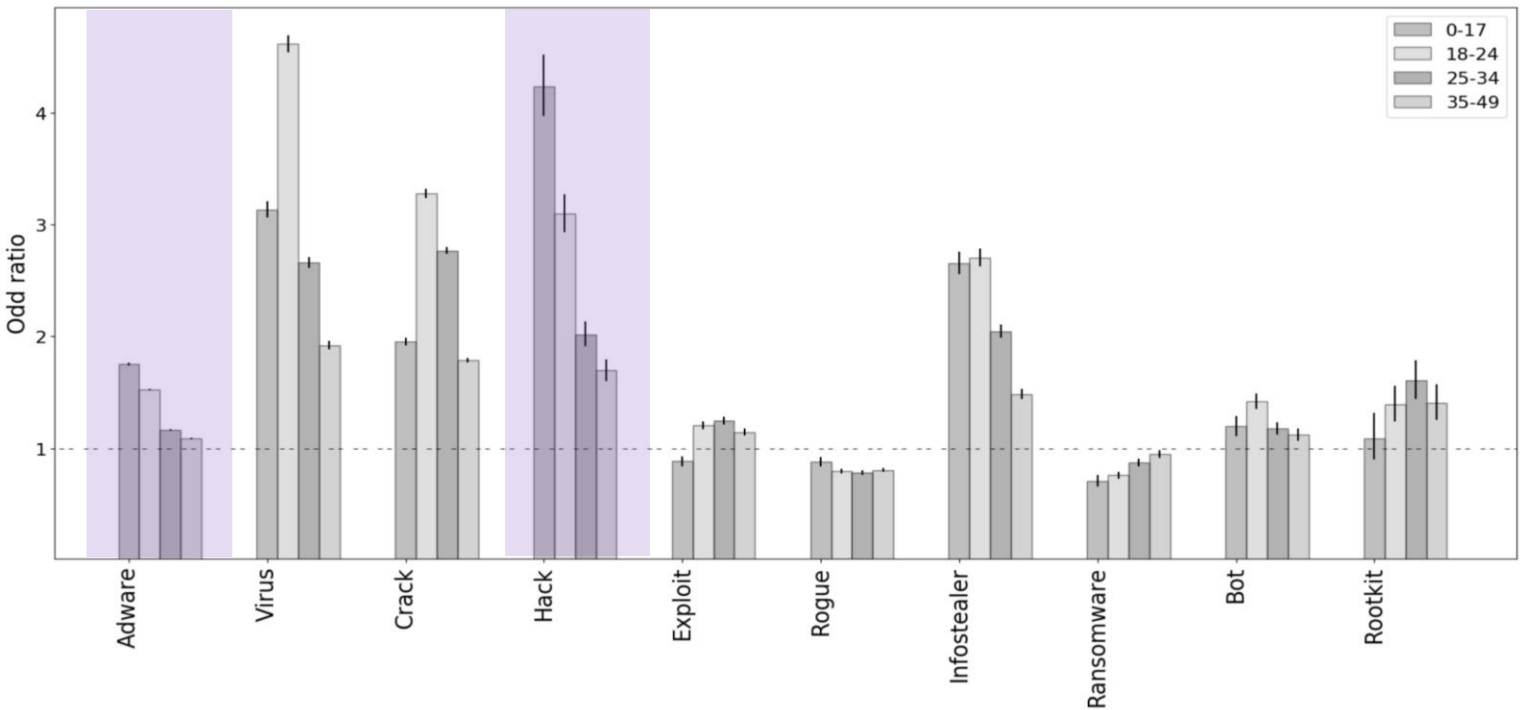
## Risk analysis of **age** by **malware types**




F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# User-level factors

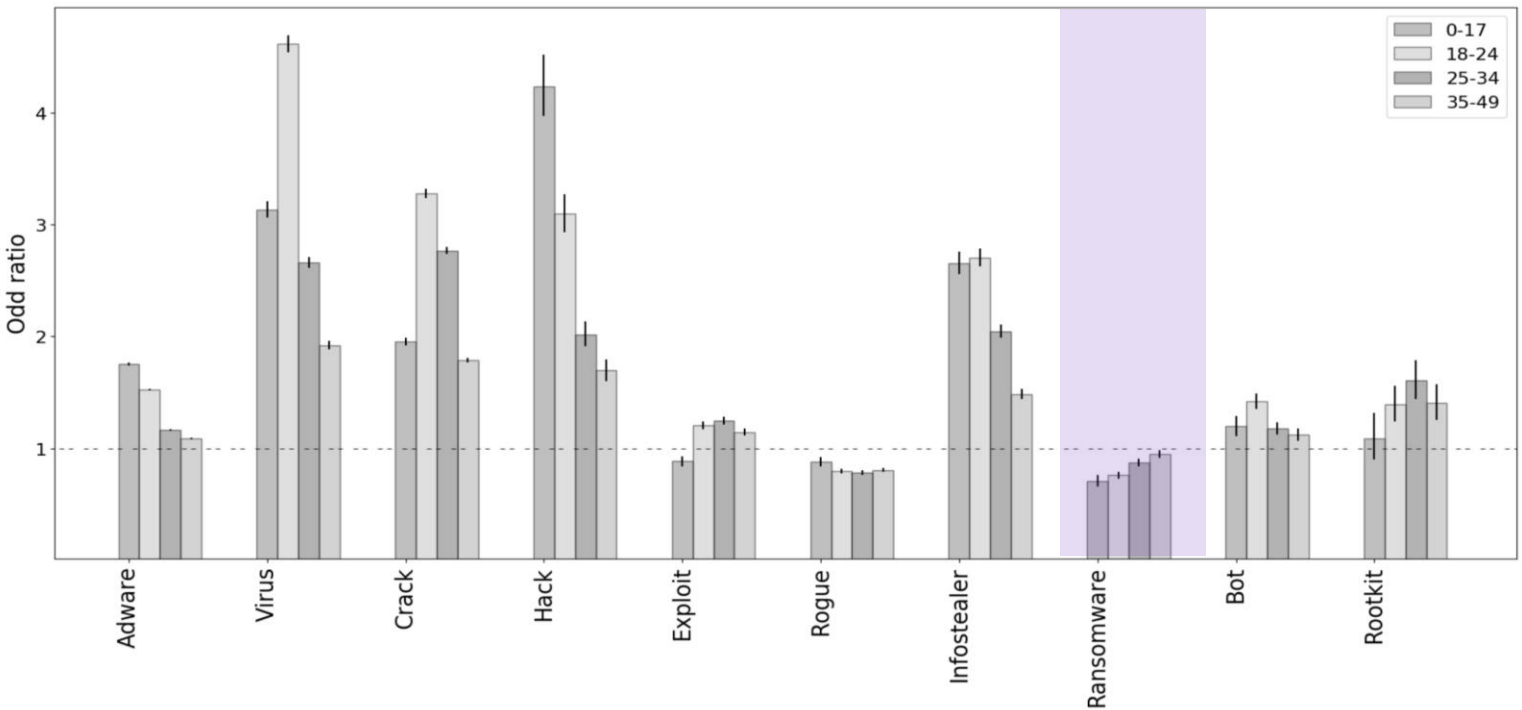
## Risk analysis of **age** by **malware types**




F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# User-level factors

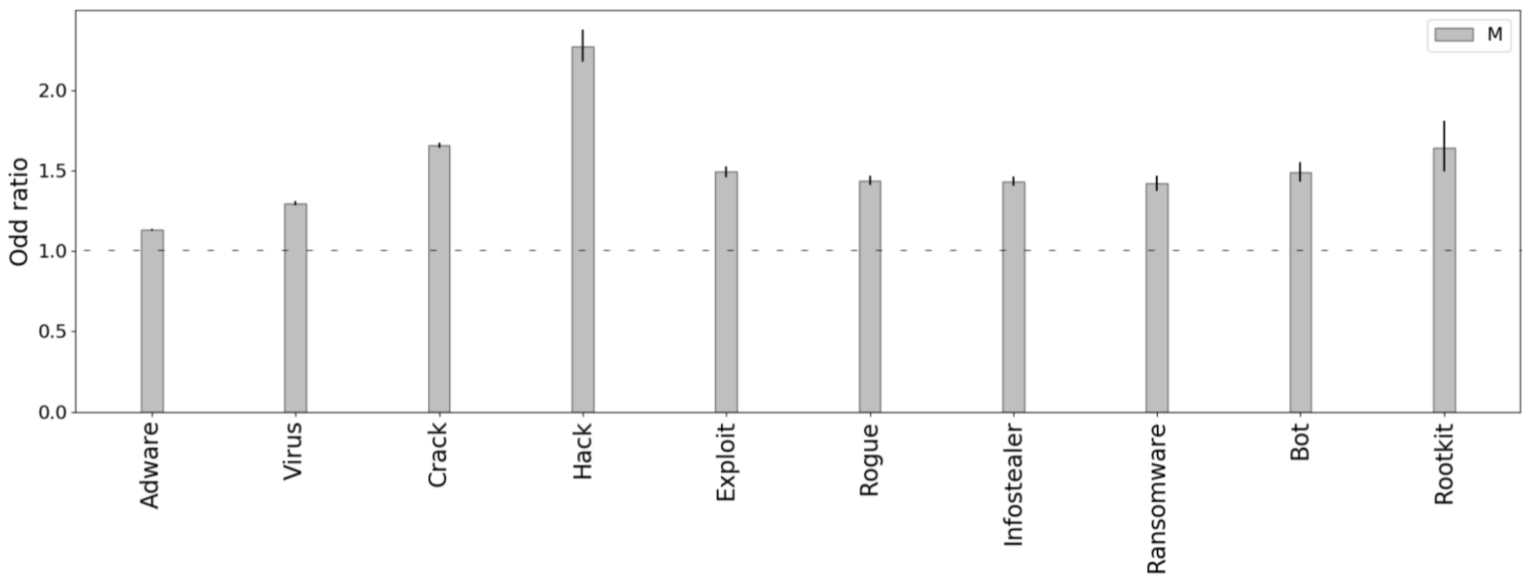
## Risk analysis of **age** by **malware types**




F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# User-level factors

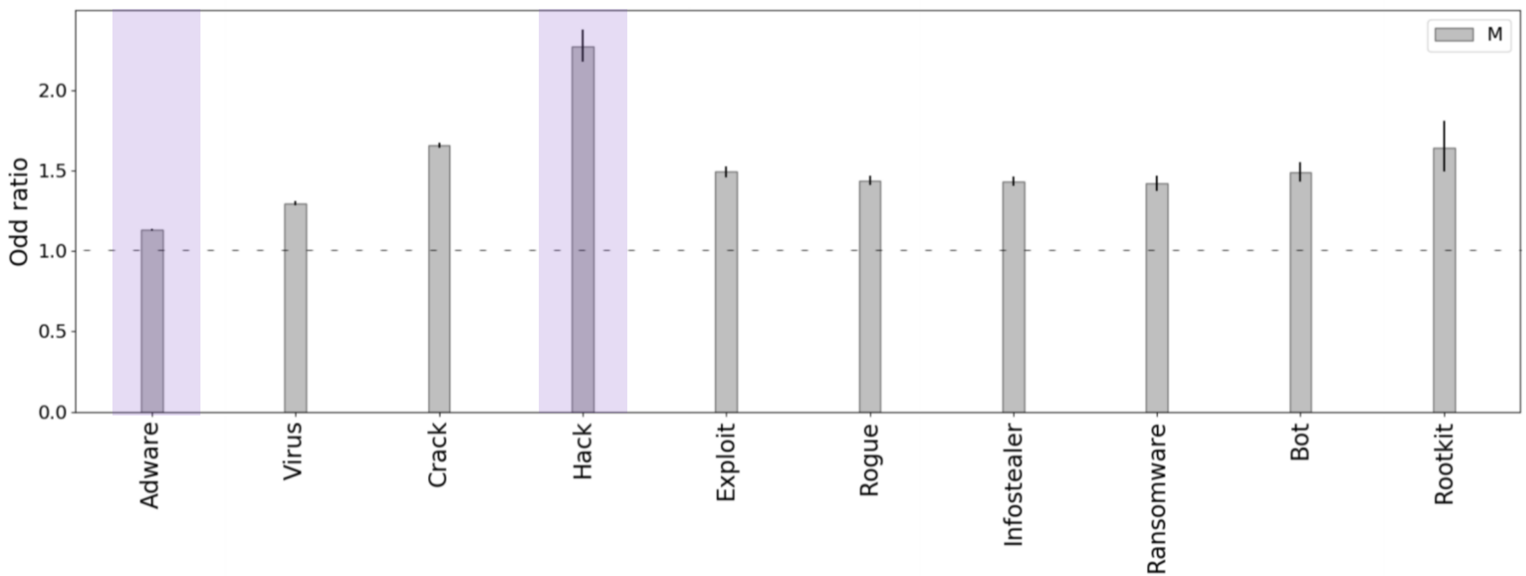
## Risk analysis of **gender** by **malware types**




F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# User-level factors

## Risk analysis of **gender** by **malware types**




F. Lalonde Lévesque et al., *Age and gender as independent risk factors of malware victimisation*, BHCI 2017.

# Findings and implications

Identification of risk and protective factors at the national and user level

Identification of *at-risk* populations

Direction and magnitude of  factors differ depending on the context

Support evidence-based decision making and prioritisation of effort

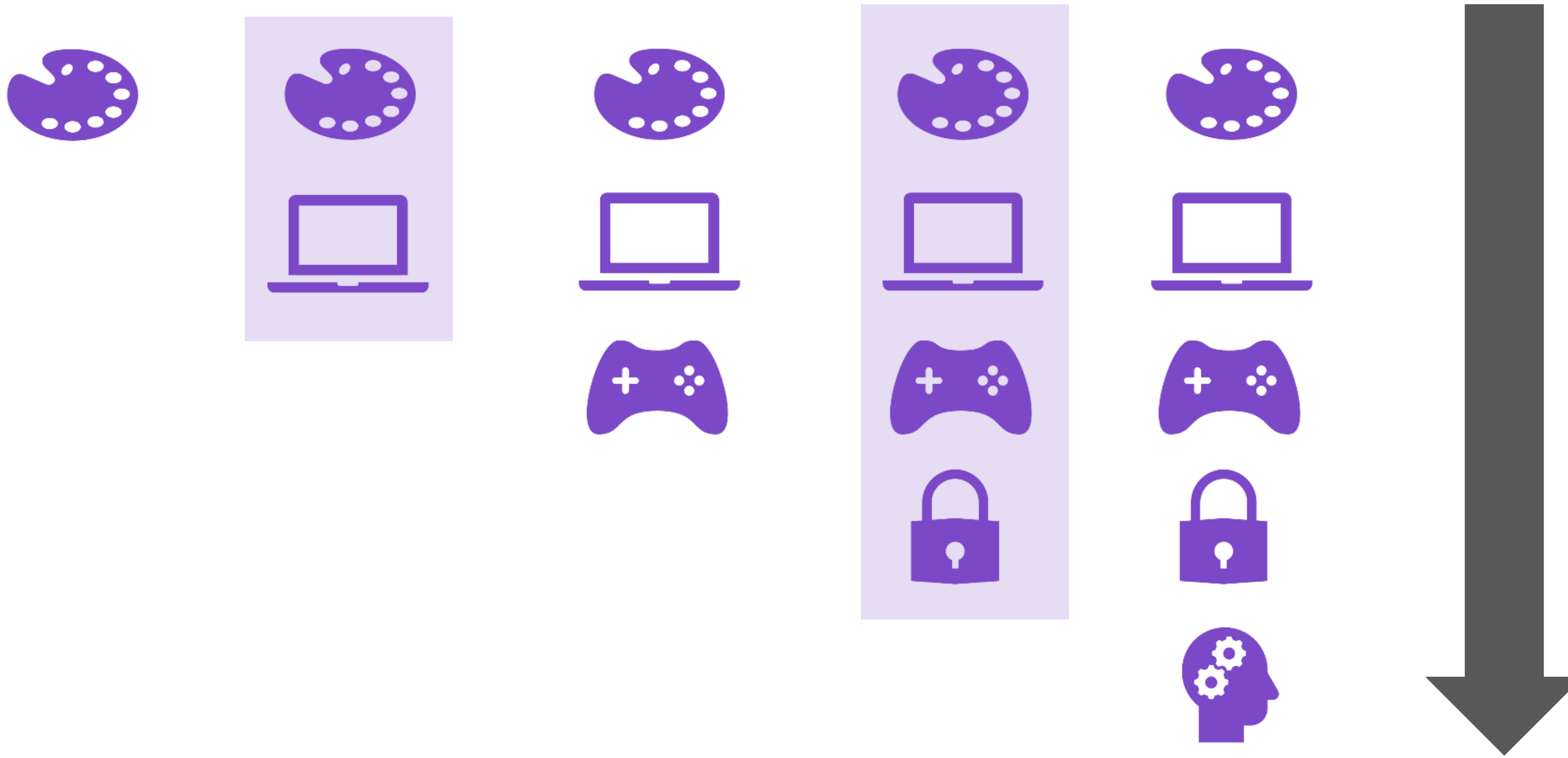
Design of targeted interventions

Development of *ecologic* strategies

# Future perspectives

- Establish sound causation
- Investigate more multi-level factors
- Extend the application of the public health model to information security

# About me...



POLYTECHNIQUE MONTRÉAL

Carleton UNIVERSITY

AppEsteem®

# Thanks !

Fonds de recherche sur la nature et les technologies Québec

NSERC CRSNG

Microsoft

ELEMENT AI

# Questions ?

Fanny Lalonde Lévesque
fanny@elementai.com