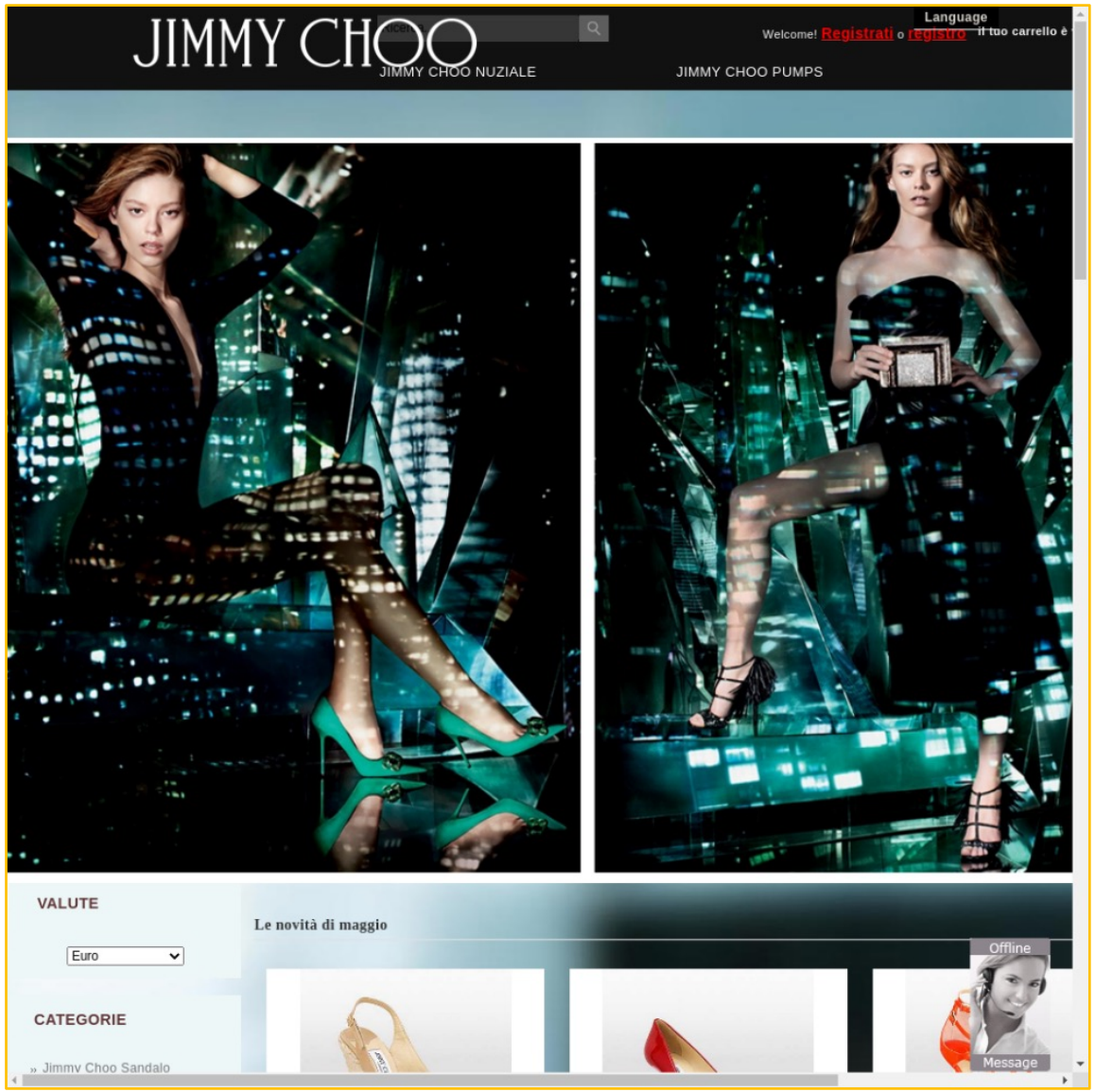
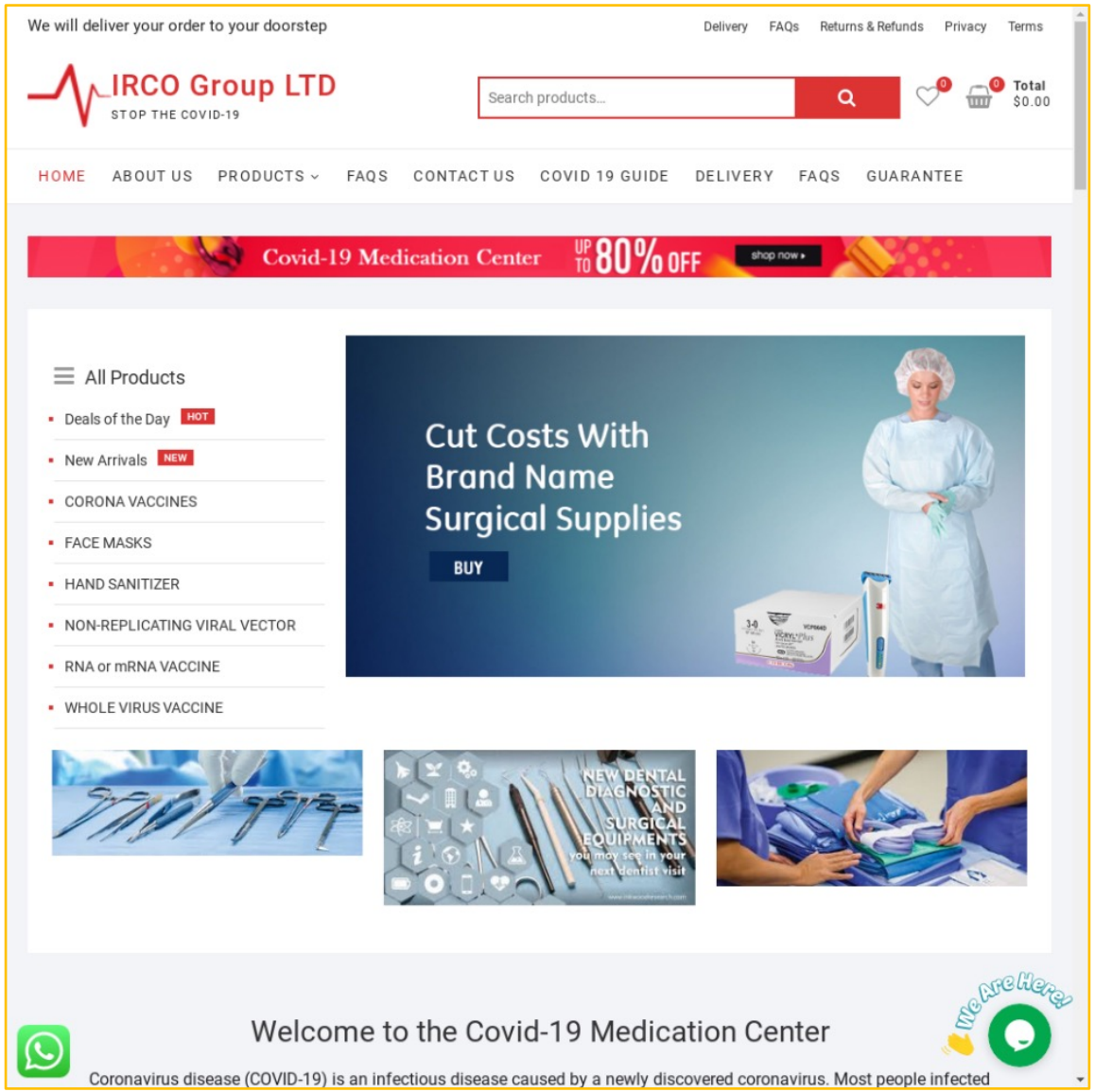
ScamMagnifier:
Detecting and Analyzing Fraudulent Shopping Websites

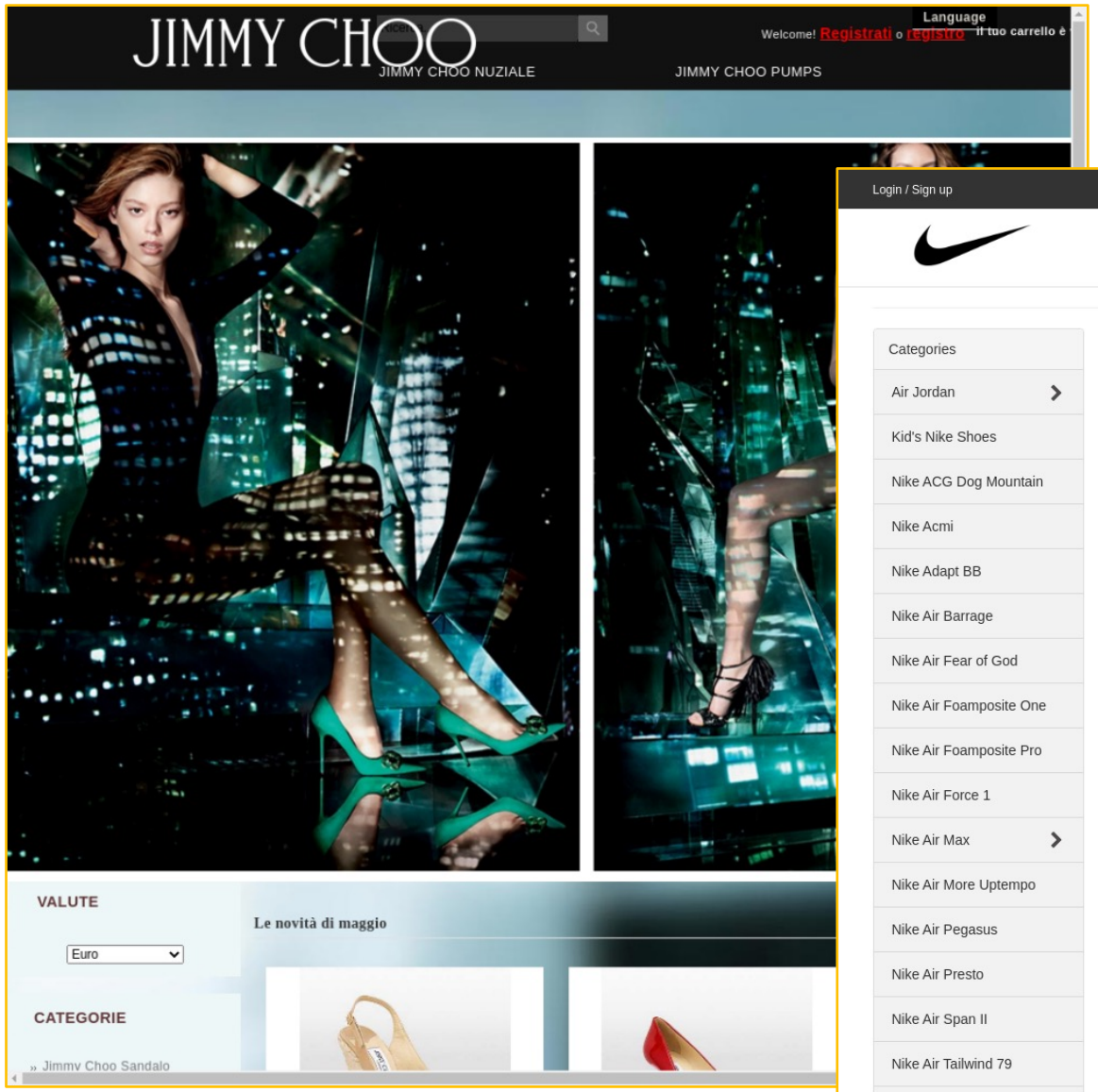
Marzieh Bitaab, Alireza Karimi, Zhuoer Lyu, Adam Oest, Dhruv Kuchhal,
Muhammad Saad , Gail-Joon Ahn, Ruoyu Wang, Tiffany Bao, Yan Shoshitaishvili, Adam Doupé

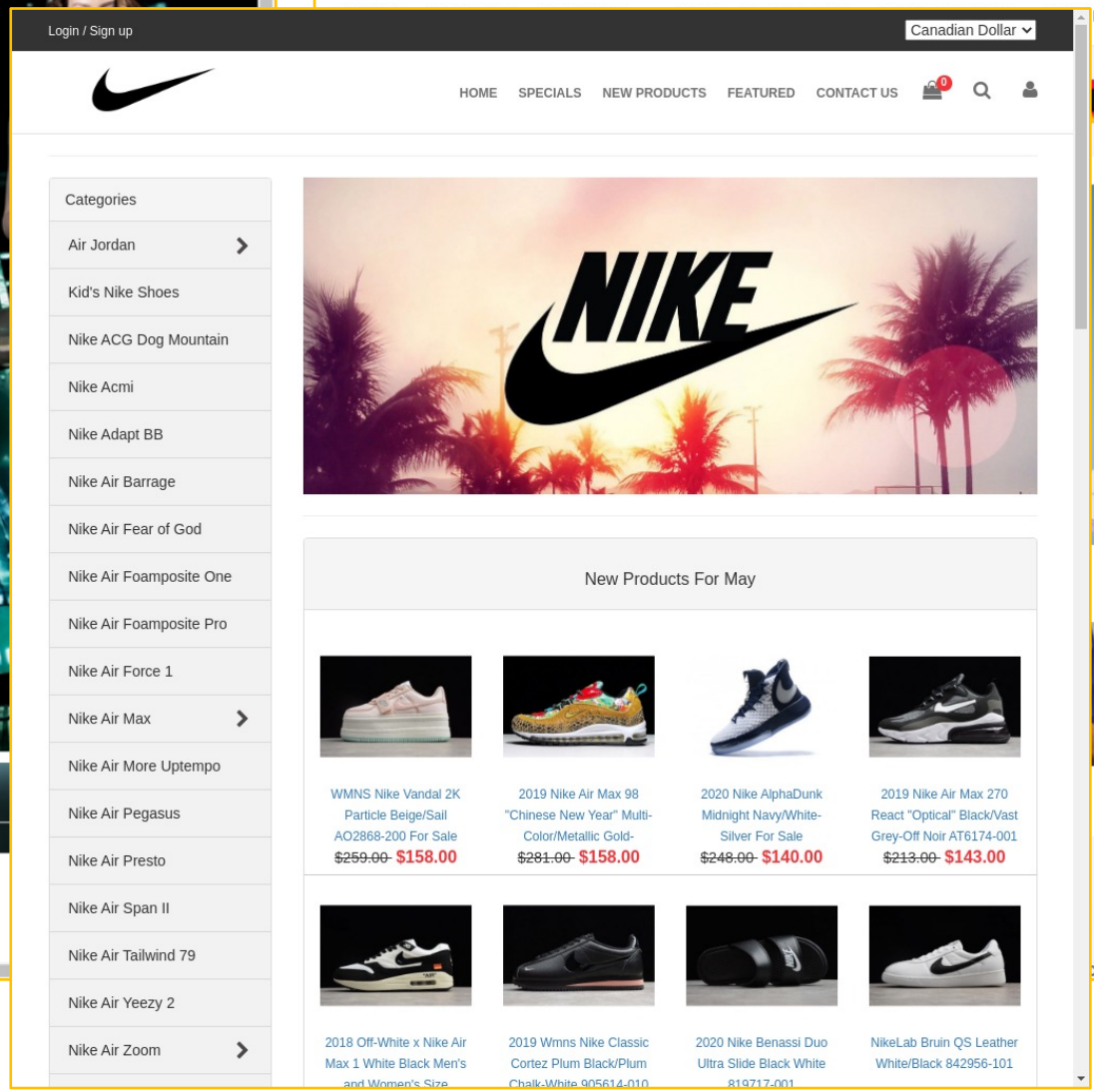
Arizona State University

sefcom
security engineering for future computing

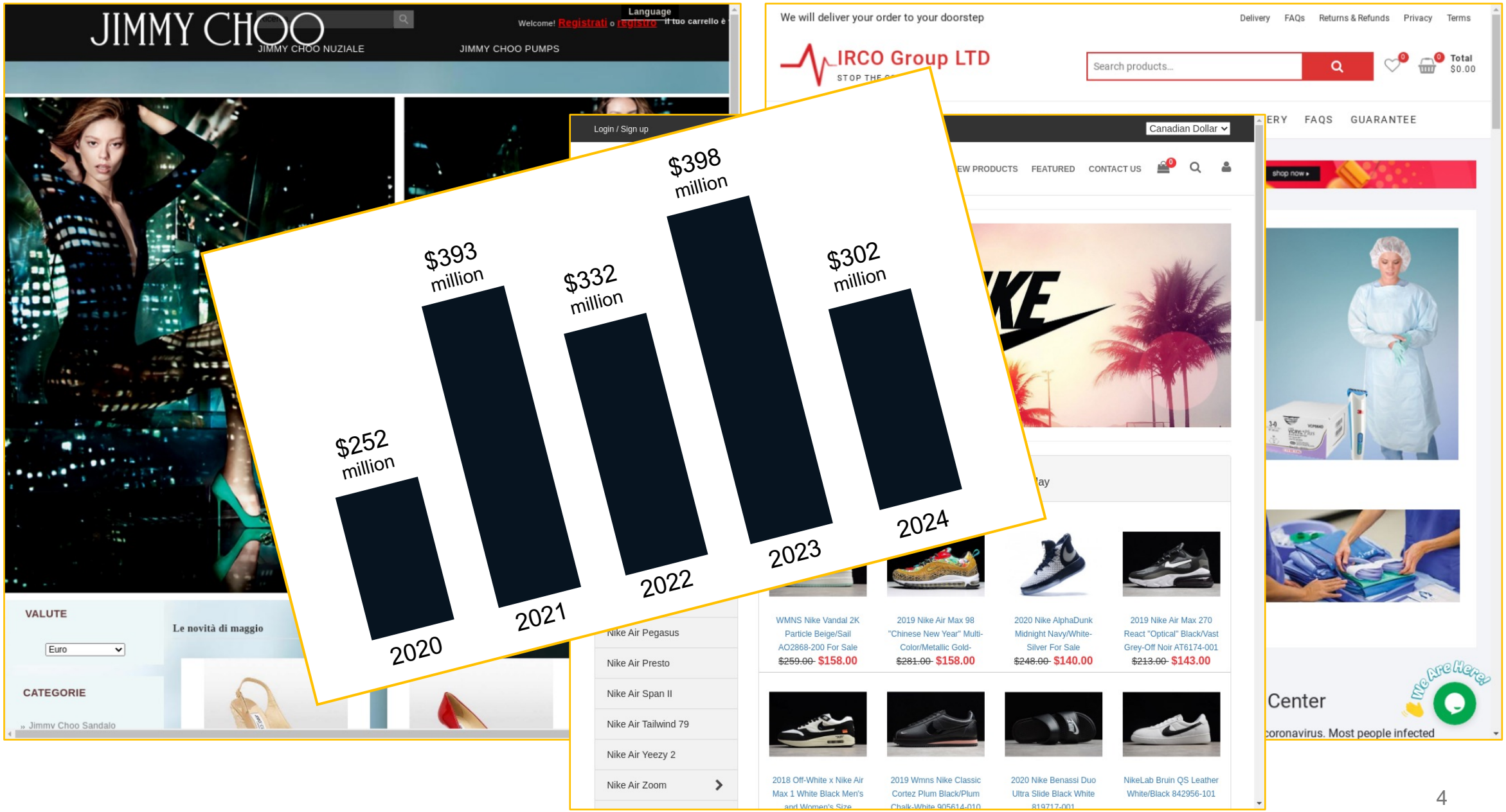

JIMMY CHOO
Language
Welcome! Registrati o registrio il tuo carrello è
JIMMY CHOO NUZIALE
JIMMY CHOO PUMPS
VALUTE
Euro
CATEGORIE
» Jimmy Choo Sandalo
Le novità di maggio
Offline
Message


We will deliver your order to your doorstep
Delivery
FAQs
Returns & Refunds
Privacy
Terms
IRCO Group LTD
STOP THE COVID-19
Search products...
Total
$0.00
HOME
ABOUT US
PRODUCTS
FAQS
CONTACT US
COVID 19 GUIDE
DELIVERY
FAQS
GUARANTEE
Covid-19 Medication Center
UP TO 80% OFF
shop now »
All Products
Deals of the Day
HOT
New Arrivals
NEW
CORONA VACCINES
FACE MASKS
HAND SANITIZER
NON-REPLICATING VIRAL VECTOR
RNA or mRNA VACCINE
WHOLE VIRUS VACCINE
Cut Costs With Brand Name Surgical Supplies
BUY
NEW DENTAL DIAGNOSTIC AND SURGICAL EQUIPMENTS
you may see in your next dentist visit
We Are Here!
Welcome to the Covid-19 Medication Center
Coronavirus disease (COVID-19) is an infectious disease caused by a newly discovered coronavirus. Most people infected


JIMMY CHOO
Language
Welcome! Registrati o registrio il tuo carrello è
JIMMY CHOO NUZIALE
JIMMY CHOO PUMPS
VALUTE
Euro
CATEGORIE
» Jimmy Choo Sandalo
Le novità di maggio


Login / Sign up
Canadian Dollar
HOME
SPECIALS
NEW PRODUCTS
FEATURED
CONTACT US
Categories
Air Jordan
Kid's Nike Shoes
Nike ACG Dog Mountain
Nike Acmi
Nike Adapt BB
Nike Air Barrage
Nike Air Fear of God
Nike Air Foamposite One
Nike Air Foamposite Pro
Nike Air Force 1
Nike Air Max
Nike Air More Uptempo
Nike Air Pegasus
Nike Air Presto
Nike Air Span II
Nike Air Tailwind 79
Nike Air Yeezy 2
Nike Air Zoom
NIKE
New Products For May
WMNS Nike Vandal 2K Particle Beige/Sail AO2868-200 For Sale
$259.00 $158.00
2019 Nike Air Max 98 "Chinese New Year" Multi-Color/Metallic Gold-
$281.00 $158.00
2020 Nike AlphaDunk Midnight Navy/White-Silver For Sale
$248.00 $140.00
2019 Nike Air Max 270 React "Optical" Black/Vast Grey-Off Noir AT6174-001
$213.00 $143.00
2018 Off-White x Nike Air Max 1 White Black Men's and Women's Size
2019 Wmns Nike Classic Cortez Plum Black/Plum Chalk-White 905614-010
2020 Nike Benassi Duo Ultra Slide Black White 819717-001
NikeLab Bruin QS Leather White/Black 842956-101

We will deliver your order to your doorstep
Delivery
FAQs
Returns & Refunds
Privacy
Terms
IRCO Group LTD
STOP THE COVID-19
Search products...
Total $0.00
ERY
FAQS
GUARANTEE
shop now »
Center
coronavirus. Most people infected


JIMMY CHOO
JIMMY CHOO NUZIALE
JIMMY CHOO PUMPS
Language
Welcome! Registrati o registro il tuo carrello è
VALUTE
Euro
CATEGORIE
» Jimmy Choo Sandalo
Le novità di maggio
$252 million
2020
$393 million
2021
$332 million
2022
$398 million
2023
$302 million
2024
Login / Sign up
Nike Air Pegasus
Nike Air Presto
Nike Air Span II
Nike Air Tailwind 79
Nike Air Yeezy 2
Nike Air Zoom
We will deliver your order to your doorstep
Delivery
FAQs
Returns & Refunds
Privacy
Terms
IRCO Group LTD
Search products...
Total $0.00
Canadian Dollar
NEW PRODUCTS
FEATURED
CONTACT US
FAQS
GUARANTEE
shop now »
WMNS Nike Vandal 2K Particle Beige/Sail AO2868-200 For Sale
$259.00 $158.00
2019 Nike Air Max 98 "Chinese New Year" Multi-Color/Metallic Gold-
$281.00 $158.00
2020 Nike AlphaDunk Midnight Navy/White-Silver For Sale
$248.00 $140.00
2019 Nike Air Max 270 React "Optical" Black/Vast Grey-Off Noir AT6174-001
$213.00 $143.00
2018 Off-White x Nike Air Max 1 White Black Men's and Women's Size
2019 Wmns Nike Classic Cortez Plum Black/Plum Chalk-White 905614-010
2020 Nike Benassi Duo Ultra Slide Black White 819717-001
NikeLab Bruin QS Leather White/Black 842956-101
Center
coronavirus. Most people infected
We Are Here!

Detecting Fraudulent Shopping Websites

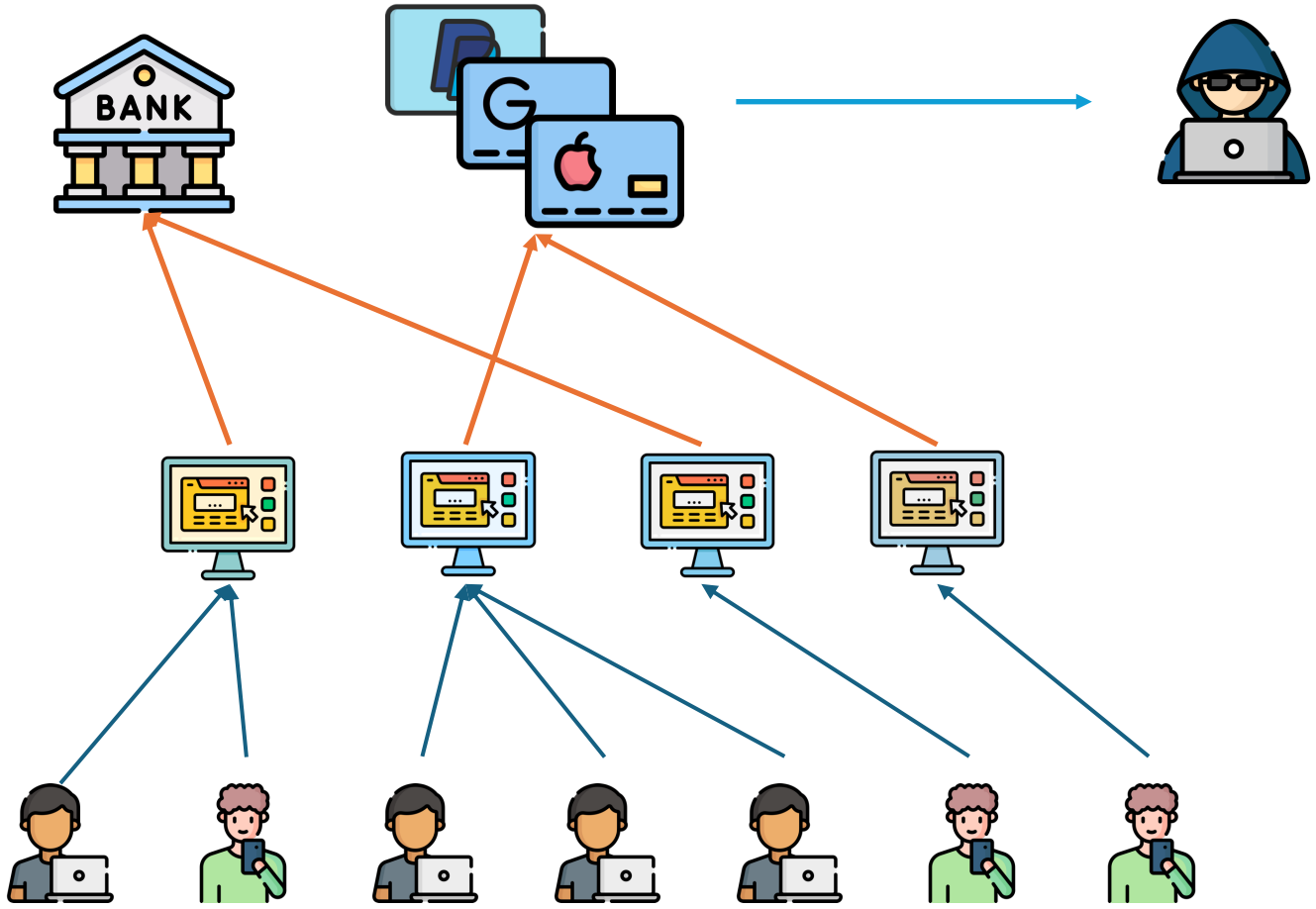
- Traditional ML approaches mostly use manually crafted features

- They struggle to keep pace with the evolving tactics

- Instead of using surface-level features, we need to dig deeper into the fraudulent shopping websites' infrastructure

- Insights from how such websites work can help future developments in detection methods

How Fraudulent Shopping Websites Work?

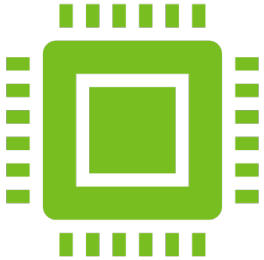


Analyzing Fraudulent Shopping Websites

Research Questions

How do fraudulent shopping websites work under the hood?

Can we pro-actively detect fraudulent shopping websites?



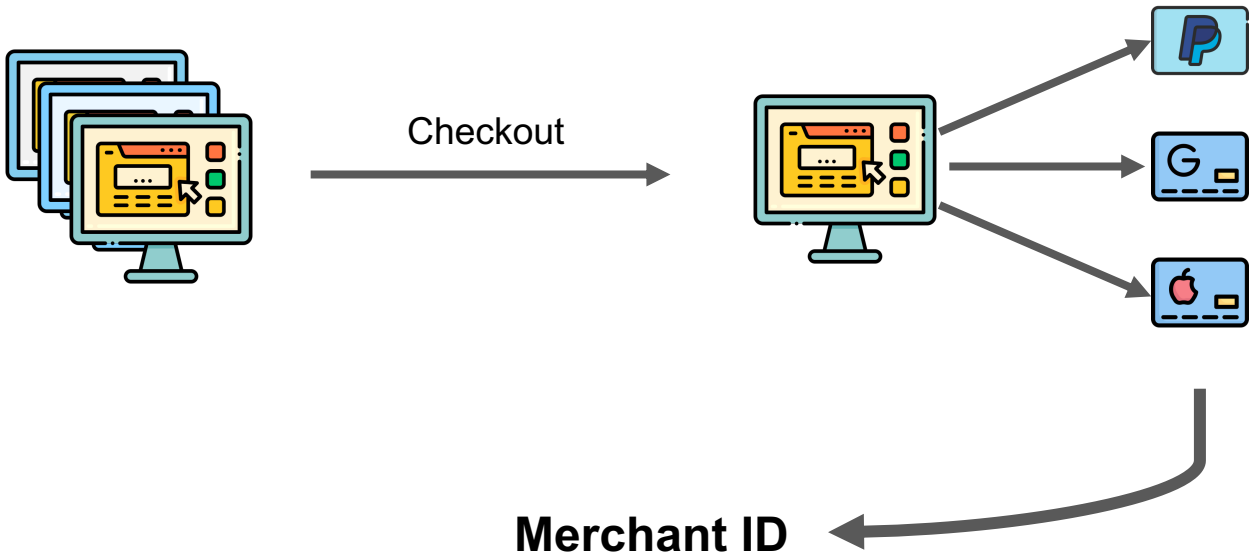
Investigation Method

Analyzing shopping websites from payment providers' point-of-view

Finding links between miscreants that create these websites

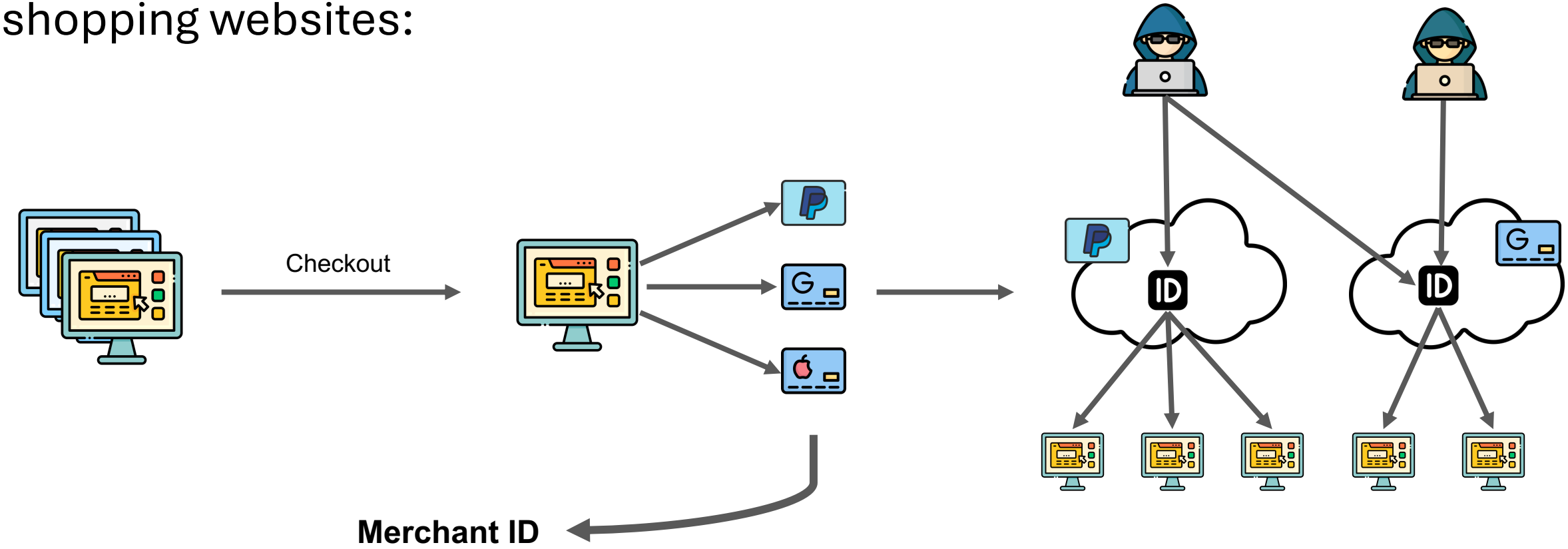
Analyzing Fraudulent Shopping Websites – Step 1: Manual Analysis

We manually analyze the process of buying items from Fraudulent Shopping Websites:



Analyzing Fraudulent Shopping Websites – Step 1: Manual Analysis

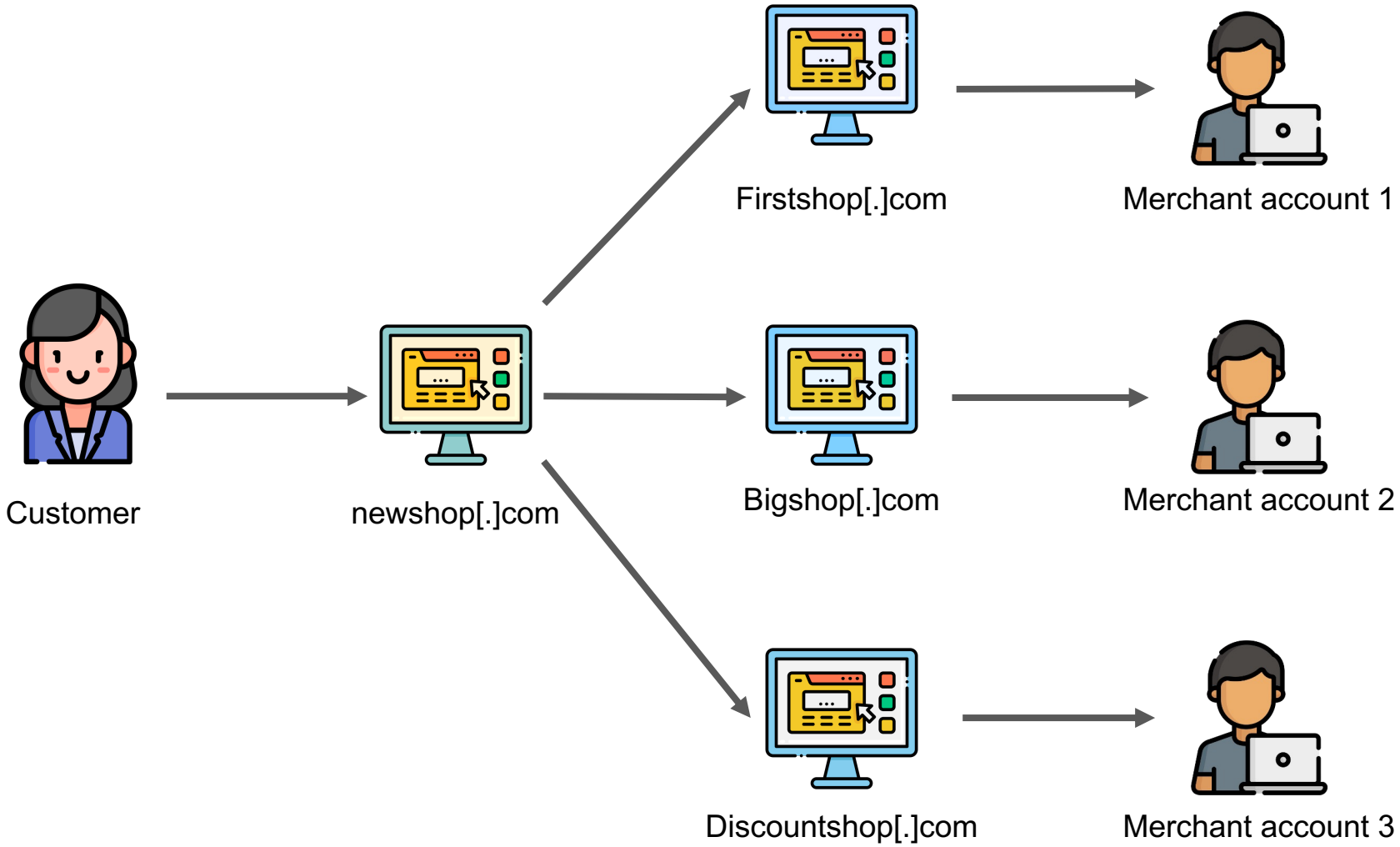
We observe that a single merchant can have multiple fraudulent shopping websites:



Merchant ID

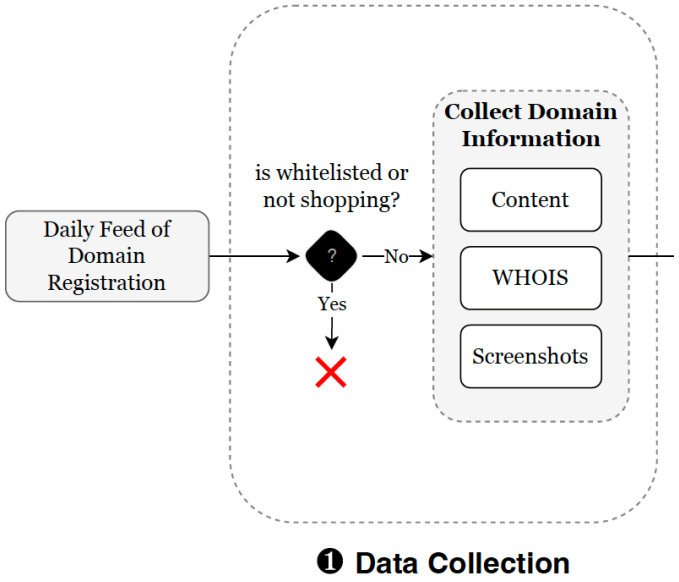
used to route payment to the website's merchant

Evasion Techniques



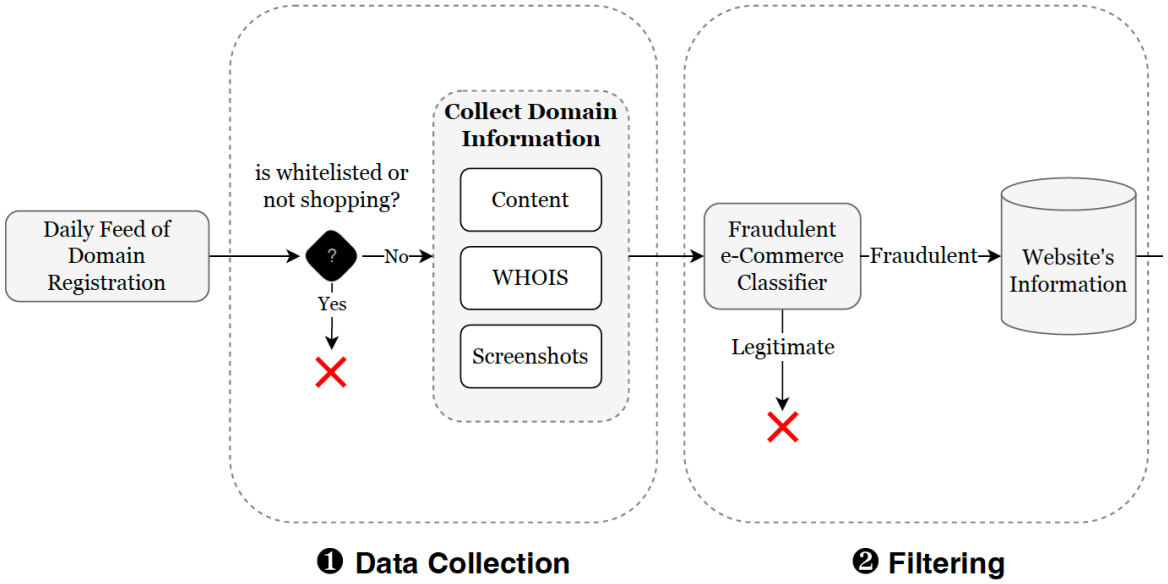
Scam Magnifier

To automate the process of data collection and analysis, we propose Scam Magnifier:



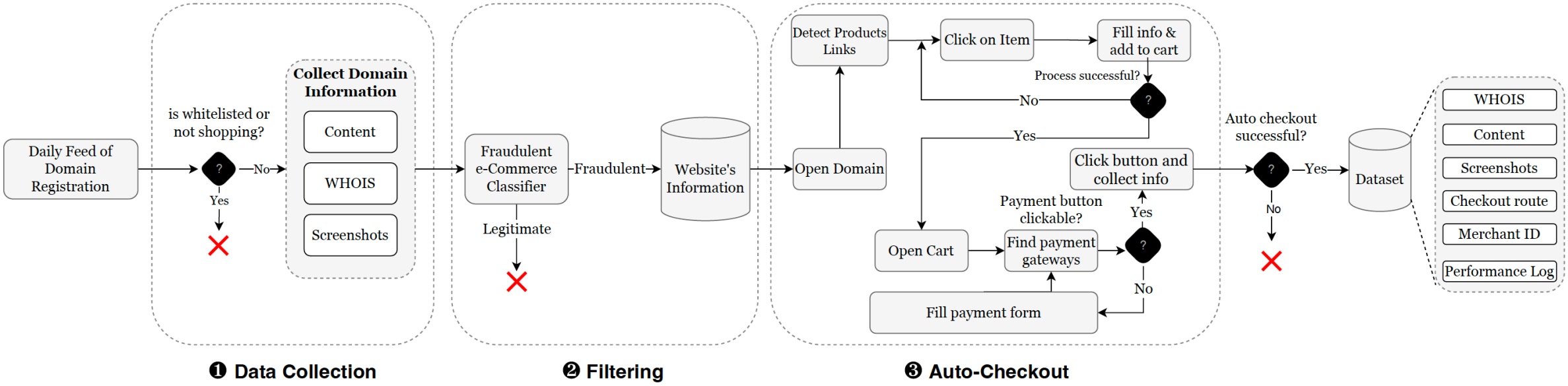
Scam Magnifier

To automate the process of data collection and analysis, we propose Scam Magnifier:

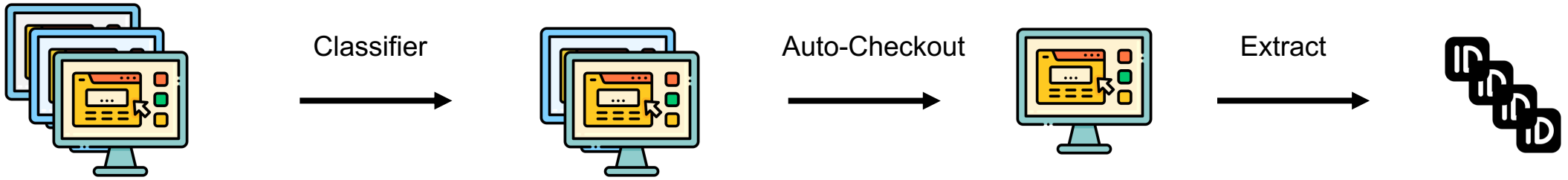


Scam Magnifier

To automate the process of data collection and analysis, we propose Scam Magnifier:

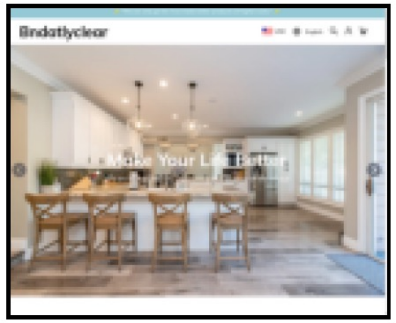


Scam Magnifier – Data Statistics

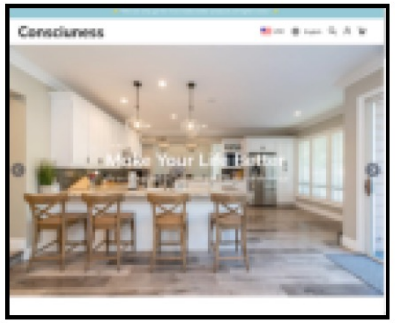


- Observations:
  - Different fraudulent websites use the same merchant ID
  - Common domain registrars and hosting providers

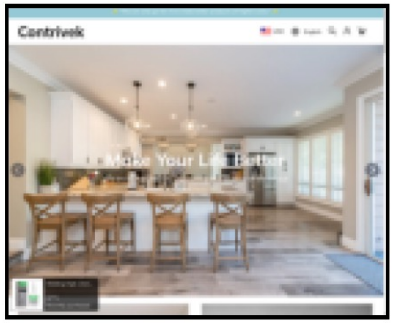
Similar Website Design



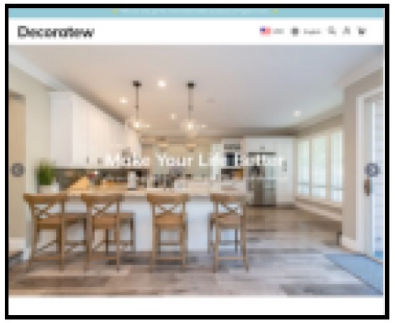
bndatlyclear.com



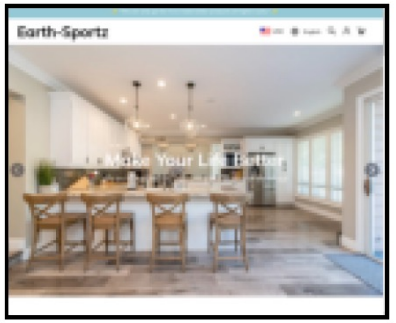
consciuness.com



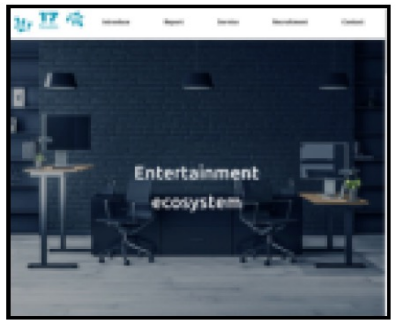
contrivek.com



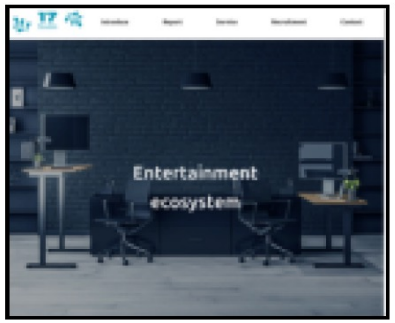
decoratew.com



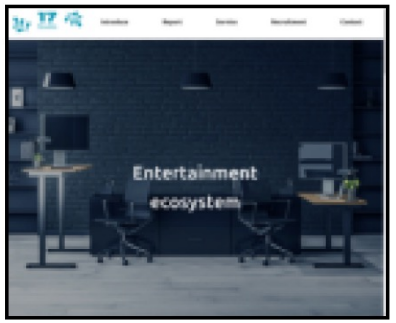
earth-sportz.co.uk



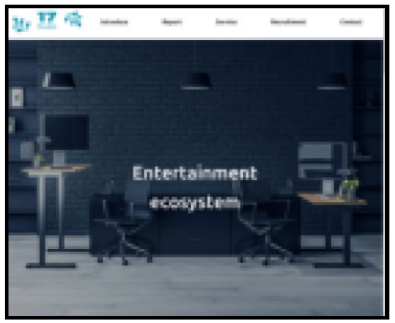
789bess.xyz



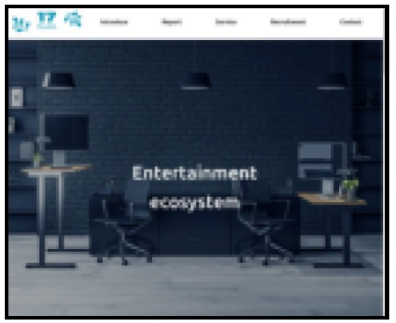
789besst.xyz



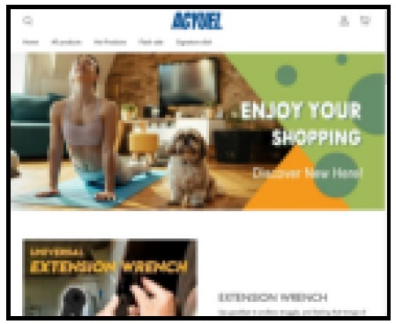
789bests.xyz



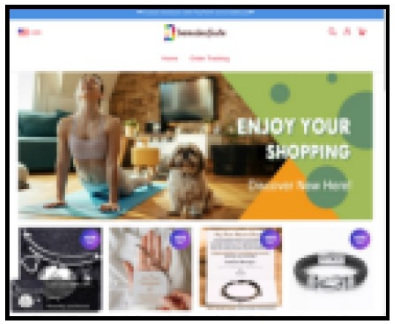
789bestts.xyz



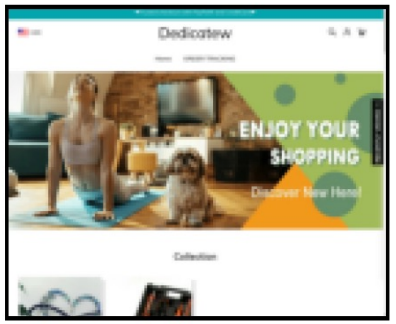
789betcom.online



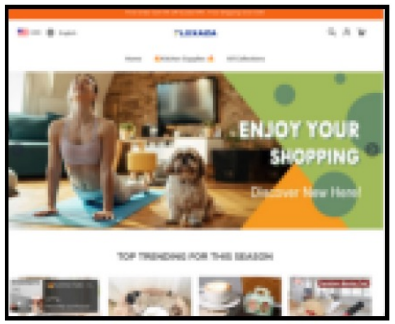
acyuel.com



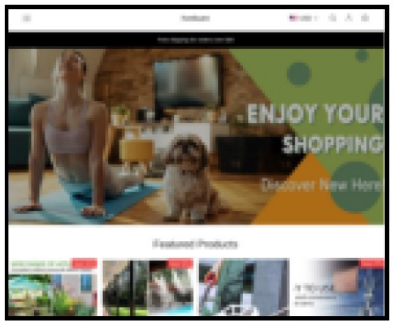
bemadeofcute.com



dedicatew.com

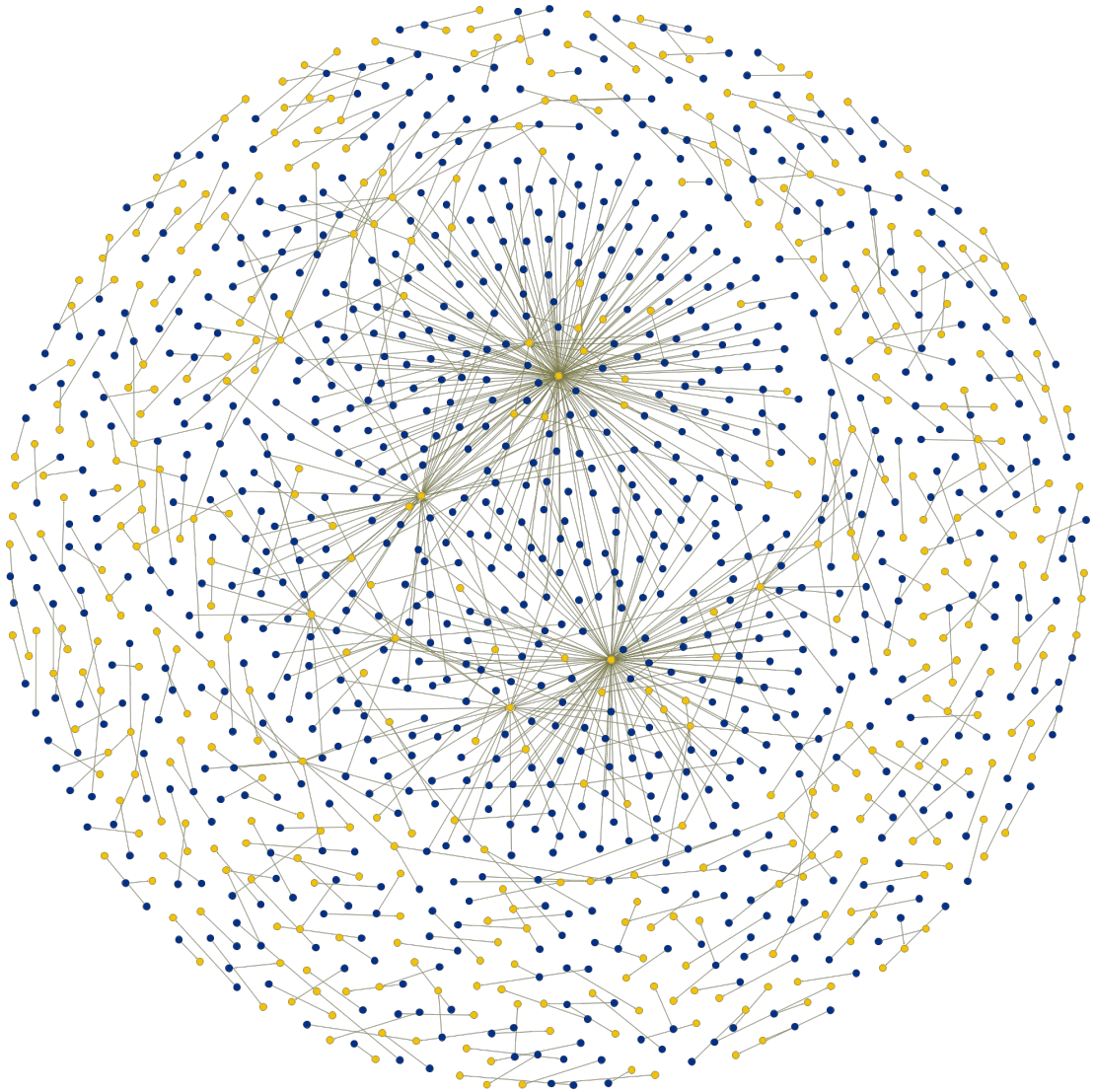


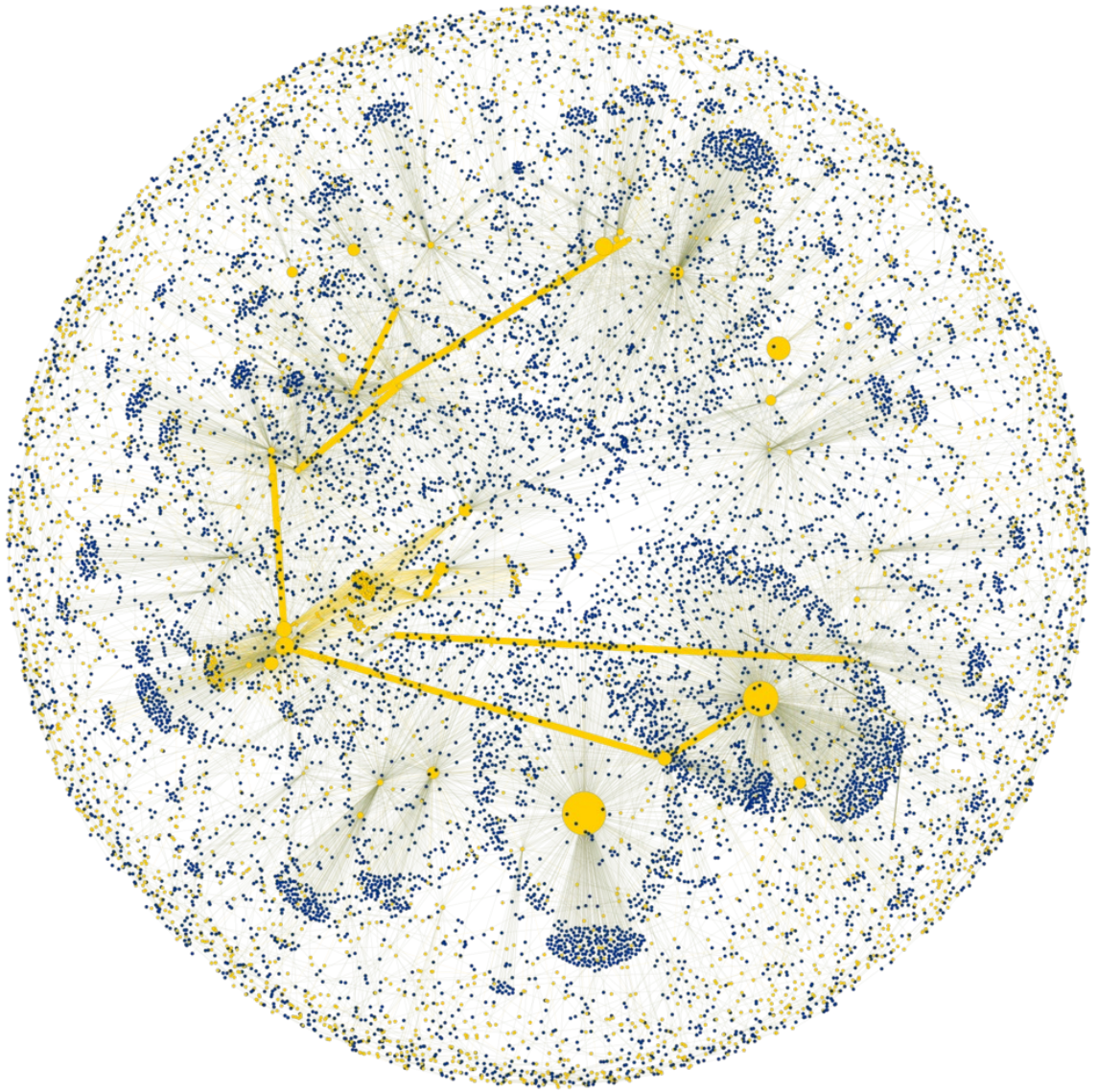
flexaza.com



hvebuen.shop

How to Link the Websites?

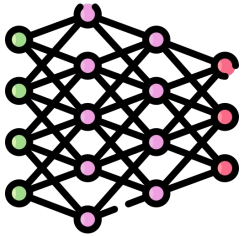




Merchants (in yellow) and their registered domains (in blue).

Takeaways

Reveals patterns of recurrence across multiple websites



Enhances response to similar threats
Preventing Financial Losses

Collaboration and data sharing between organizations
Blocklisting or flagging future transactions

Marzieh Bitaab
mbitaab@asu.edu