Ctrl+Alt+Deceive: Quantifying the Impact of Online Scams on End Users

Platon Kotzias (BforeAI), Michalis Pachilakis (Norton Research Group), Javier Aldana Iuit (Norton Research Group), Juan Caballero (IMDEA Software Institute), Iskander Sanchez-Rola (Gen Innovation), Leyla Bilge (Norton Research Group)

Impact of scams on Internet users

Emotional Distress

- Feelings of betrayal, embarrassment, and vulnerability

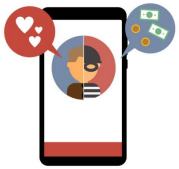
Financial Losses

- FTC reported $10 billion in losses for 2023
- ACCC $455M in losses for 2023

Prior work

Tech Support

Cryptocurrency



Romance

Survey

NFT

Pet

Shopping

Defenses against specific scam types

Consumer Agencies Reports

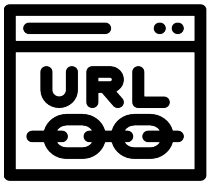
Research Questions

- What is the overall user exposure to scams?
- What scam types are users most exposed to?
- What is the lifetime of scams?
- What fraction of scams are reached through online ads?
- Are there geographical differences among scams?
- What fraction of users are scammed?

Datasets

Telemetry

11M
Windows desktop devices
(IP addresses)



196.9 billion
browser URL visits
(benign + malicious)

232 country codes

14M
Android/iOS devices
(IP addresses)

112.2 billion
domain visits
(benign + malicious)

Scam Domains

SCAMADVISER

341K scam FQDNs
(after filtering)

289K FQDNs
shopping scams

Total of 607.2K scam FQDNs
from 501.7K SLDS

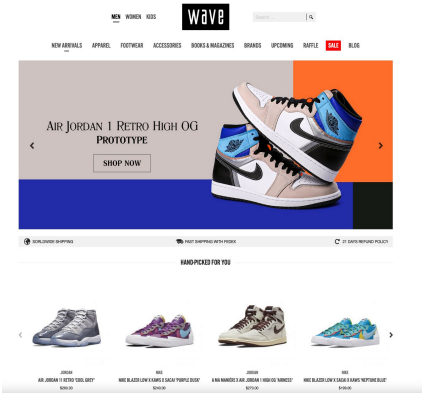
Scam Classification

- Leverage content signatures from ScamAdviser feed
- Evaluate per-tag precision
- Can be applied directly to the telemetry data

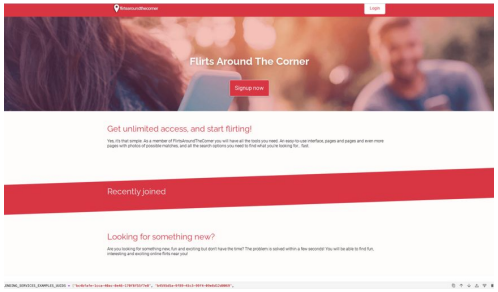
ScamAdviser Industry Tag	Domains	Prec.	Scam Type
Essay/Thesis/Dissertation Writers	323,060	0%	✗
Shopping	191,918	72%	Shopping
Cryptocurrency	90,873	80%	Cryptocurrency
Hacking - High Risk	72,264	0%	✗
Media - Games	65,658	12%	✗
Financial Service - Very High Risk	60,159	77%	Financial
Financial Services - High Risk	50,847	87%	Financial
Financial Services - HYIP	28,906	89%	Financial
Media - Movies	28,568	31%	✗
Gambling	18,453	90%	Gambling
Adult	17,209	26%	✗
Financial Services	13,825	100%	Financial
Media - Software	10,659	39%	✗
Sport Betting	10,229	58%	✗
Non-Profit Organization	9,924	24%	✗
Media - Books	8,225	27%	✗
Media Subscription Services	6,723	30%	✗
Adult - Dating	6,399	86%	Dating
File Sharing Service	5,943	27%	✗
Jobs	4,914	72%	Employment
Travel Services	3,290	65%	✗
NFTs	2,762	40%	✗
Recovery Services	1,331	84%	Funds recovery
Visa Services	1,121	66%	✗
Lending Service	432	62%	✗
Helpdesk - IT Support	406	40%	✗

This process outputs 7 scam types

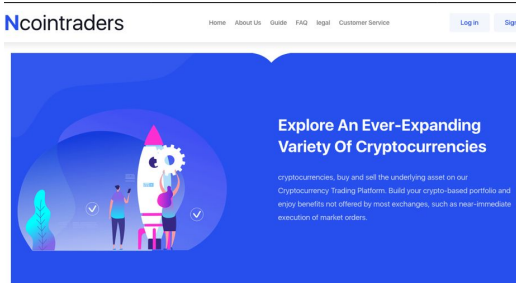
Scam Types



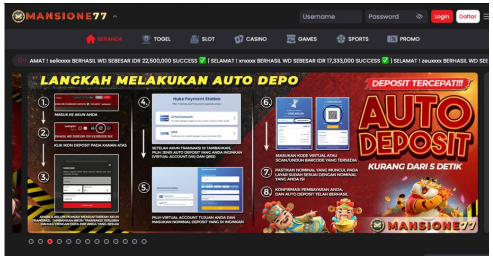
Shopping



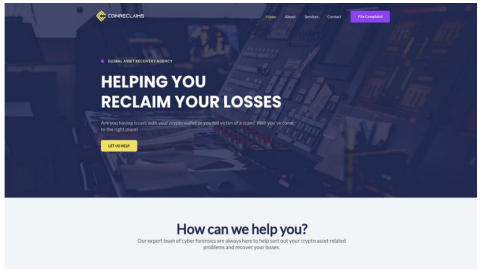
Dating



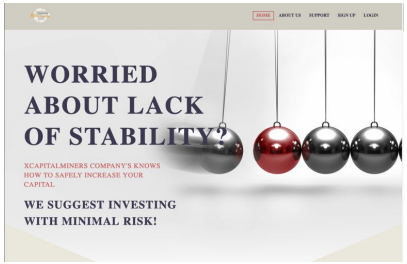
Cryptocurrency



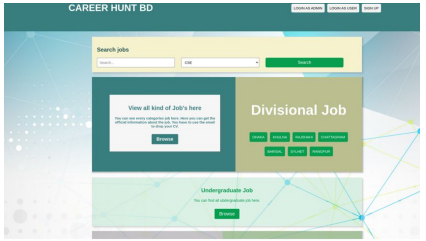
Gambling



Funds Recovery



Financial



Employment

What is the overall user exposure to scams?

- **82.7% (414K)** scam SLDs are observed in the telemetry
- **25.1M** desktop + mobile IP addresses visit the scam sites

Daily Stats	Median	Mean	Stdev	Min	Max
Desktop	**101K**	101.7K	20K	61.9K	145.5K
Mobile	**48K**	37.3K	23.8K	9.1K	71.6K

Each day over 149K devices are exposed to online scams

What scam types are users most exposed to?

Scam Type	SLDs	IPs
Shopping (All)	288.2K (71.7%)	10.2M
Shopping (ScamAdviser)	30.0K (7.5%)	2.8M
Cryptocurrency	7.2K (1.8%)	652.9K
Financial	5.6K (1.4%)	442.8K
Dating	348 (0.1%)	177.8K
Gambling	858 (0.2%)	54.9K
Employment	651 (0.2%)	49.2K
Funds Recovery	51 (<0.1%)	25.6K
Unclassified	*98.9K (24.6%)*	*10.7M*
All	***402.2K (100%)***	***20.4M***

Desktop Telemetry

Scam Type	SLDs	IPs
Shopping (All)	77.8K (69.9%)	2.9M
Shopping (ScamAdviser)	20.0K (18.0%)	1.5M
Cryptocurrency	1.4K (1.2%)	50.9K
Financial	957 (0.9%)	20.4K
Dating	176 (0.2%)	13.3K
Gambling	170 (0.2%)	3.3K
Employment	134 (0.1%)	2.1K
Funds Recovery	12 (<0.1%)	438
Unclassified	*32.9K (29.6%)*	*2.0M*
All	***111.3K (100%)***	***4.7M***

Mobile Telemetry

Users are most exposed to shopping scams followed by cryptocurrency and financial scams

What is the lifetime of scams?

Scam Type	Active Time Med	Active Time Mean	Listing Delay Med	Listing Delay Mean	Wait Time Med	Wait Time Mean
Dating	59	75.2	8	25.3	19	20.9
Shopping	15	42.6	1	11.3	24	43.2
Employment	4	31.7	14	34	9	21.7
Gambling	3	37.9	4	24.7	10	11.6
Funds recovery	1	42.6	2	29.5	29	29.6
Financial	1	32.0	1	-0.6	22	41.2
Cryptocurrency	1	25.9	1	-0.3	11	30.8
Unclassified	3	27.2	5	22.5	5	16.4
All	11	38.7	1	13.8	18	36.5

- Lifetime measurements cover both desktop and mobile telemetry
- **Active time** → Time difference between the first and the last observations of an SLD in the telemetry

Scam domains remain active 12-15 times longer than phishing domains (17h-21h)

What is the lifetime of scams?

Scam Type	Active Time Med	Active Time Mean	Listing Delay Med	Listing Delay Mean	Wait Time Med	Wait Time Mean
Dating	59	75.2	8	25.3	19	20.9
Shopping	15	42.6	1	11.3	24	43.2
Employment	4	31.7	14	34	9	21.7
Gambling	3	37.9	4	24.7	10	11.6
Funds recovery	1	42.6	2	29.5	29	29.6
Financial	1	32.0	1	-0.6	22	41.2
Cryptocurrency	1	25.9	1	-0.3	11	30.8
Unclassified	3	27.2	5	22.5	5	16.4
All	11	38.7	1	13.8	18	36.5

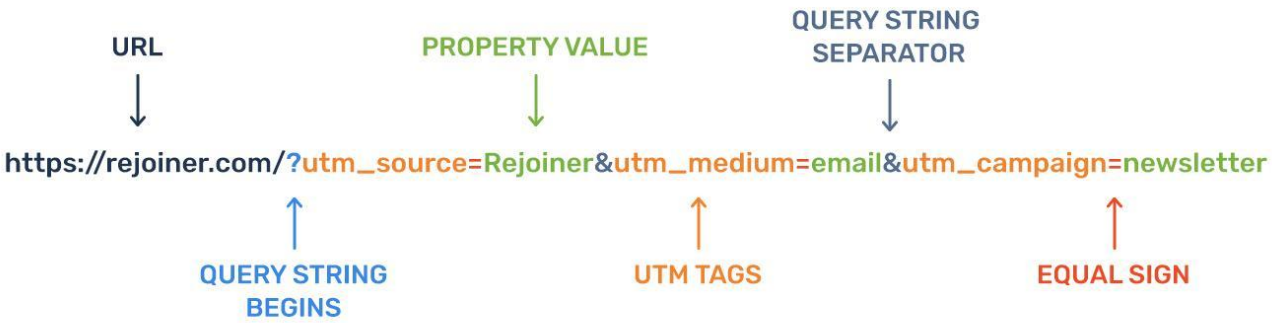
Listing delay → Time difference between the first observation of the SLD in the telemetry and the first appearance of the domain in a scam domain feed

- 7.9% of scams are identified before users visit them
- Scams receive 58.6% of their traffic within the first day

Scam domains are observed in telemetry a median of 1 day before they are listed in a scam feed

What fraction of scams are reached through online ads?

- Leverage Urchin Tracking Module (UTM) parameters in scam URLs of desktop telemetry
- Added by scammers for tracking their scam advertising campaigns



What fraction of scams are reached through online ads?

Scam Type	Observations	SLD	IP
Shopping	6,615,332 (20.6%)	32,901 (11,4%)	2,337,930 (22.9%)
Cryptocurrency	349,168 (13.0%)	340 (4.7%)	131,611 (20.1%)
Financial	46,367 (2.6%)	302 (5.3%)	22,498 (5.1%)
Funds recovery	250 (0.5%)	5 (9.8%)	184 (0.7%)
Gambling	659 (0.4%)	32 (3.7%)	276 (0.5%)
Employment	310 (0.3%)	32 (4.9%)	208 (0.4%)
Dating	7,335 (0.2%)	108 (31.0%)	138 (<0.1%)
Unclassified	*2,086,766 (7.1%)*	*5,179 (5.2%)*	*826,973 (7.7%)*
All	***9,231,334 (13.3%)***	***38,982 (9.7%)***	***3,127,873 (15.3%)***

- Shopping and cryptocurrency scams are the most advertised (and attract most visits)
- Cryptocurrency ads are more successful

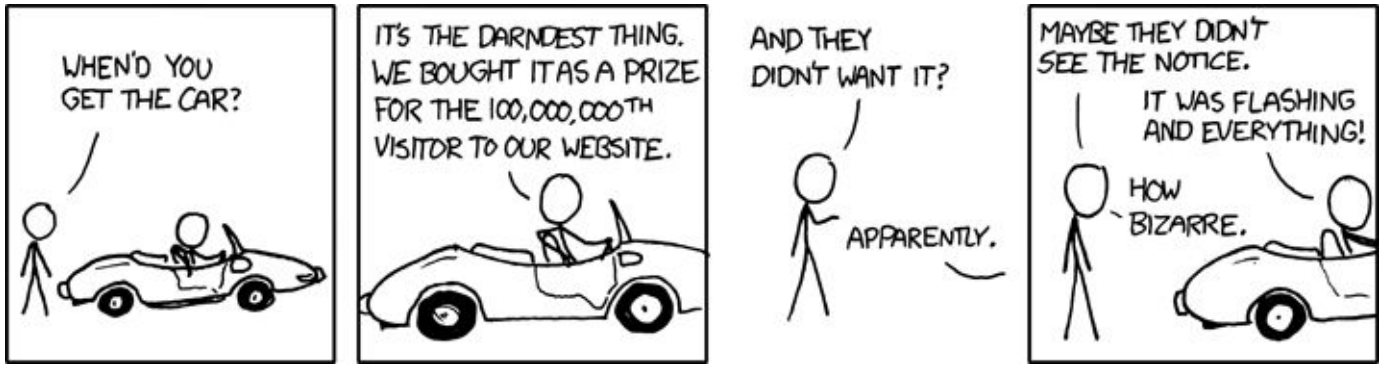
In 13.3% of all scam observations users followed an advertisement

Top advertising sources of online scams

Source	Observations
Facebook	4,948,800 (75.1%)
X (former Twitter)	503,259 (7.6%)
Newsletter	66,710 (1.0%)
Taboola	65,830 (1.0%)
Copernica	24,649 (0.4%)
Shopify	9,371 (0.1%)
All	***6,592,206 (100%)***

- Focus on 6.5M scam observations that include a UTM source parameter

Scam advertisements are placed largely on social media, most often on Facebook



Thank you!

Contact: platon@bfore.ai