SECURITY (COMP0141): ABUSE FOR PROFIT

UCL

WHAT DOES MALWARE DO?

What is the point of spreading malware?

Financial motivation:

- expand botnet (A)
- steal information like credentials (CIA)
- ransomware (A)

Political motivation:

- state-level attacks (cyber warfare) (CIA)

REPORTED INTERNET CRIME

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

REPORTED INTERNET CRIME

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

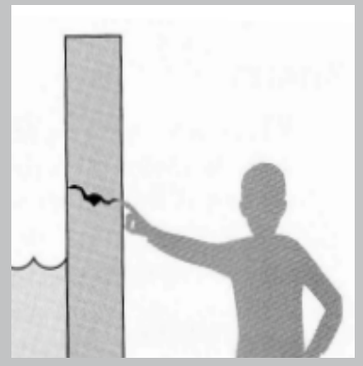
FINANCIALLY MOTIVATED ABUSE

DoS, botnets, and malware all require a high degree of technical sophistication

Much easier: **run a scam**

motivation: money

capabilities: limited



vulnerability: us!

human behaviour, weakness, etc.

EXERCISE

how could these platforms be abused for profit?

how could you prevent it from happening?

FINANCIALLY MOTIVATED ABUSE

Social media: spammer accounts, promotional accounts

Messaging apps: spammer accounts, promotional accounts

App stores: SEO, bad apps

Airbnb: scam rentals

TripAdvisor: fake reviews, fake restaurants

Uber: colluding drivers

Dating apps: spammer accounts, romance scams

DETECTING SPAM

Spam is all about operating in **bulk**: even if the chance of a click is only 0.0001%, can still get thousands of clicks with billions of emails

This makes it possible to have highly effective spam classifiers

- patterns across sent/received emails (if large provider)
- how many links are embedded?
- do you know the sender?
- huge volume of training data for ML classifiers

CONFIDENCE FRAUD / ROMANCE

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

DATING SCAMS

Spam is all about operating in **bulk**: even if the chance of a click is only 0.0001%, can still get thousands of clicks with billions of emails

Need to access spam recipients: an email address
Need to access dating apps: a (mostly) realistic account

This is a lot more work to create!

DATING SCAMS

Spam is all about operating in **bulk**: even if the chance of a click is only 0.0001%, can still get thousands of clicks with billions of emails

Need to access spam recipients: an email address
Need to access dating apps: a (mostly) realistic account

So, scams are often much more **targeted**

Do also see spam, promotions, etc. but these can be detected using the same techniques as for normal spam

DATING SCAMS

“Hi Bob! 😊”

❤️

…talk for hours…

😕

“my camera is broken 😢”

“I live in another country but
I want to come live with you”

❤️

…

💸

“Could you pay for my visa?”

DETECTING DATING SCAMS

This is much harder than for spam because:

- unsolicited messages are the point of a dating app
- the target is a willing participant
- interactions quickly move off the platform
- scam interactions are designed to resemble normal ones

Still, we can try to look for:

- key things missing in a profile
- higher representation of niche traits (e.g., widowed)
- altered, repurposed, or repeated images

ADVANCED FEE FRAUD

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

ADVANCED FEE FRAUD

"Hi Bob! I need your help."

...talk for a bit...

"If you just give me X
I will give you Y in return."
(where Y ≫ X)

Also known as:

- Spanish Prisoner scam (dates back to early 1800s)
- Previously called a 419 scam

ADVANCED FEE FRAUD DEMO

Steve Hailes <stevehailes428@gmail.com>
to S.Meiklejohn@cs.ucl.ac.uk

Are you available at the moment,

Best Regards,
Head of department,
Steve.

HONEYPOTS

A **honeypot** is designed to be highly attractive to an attacker

- unlocked car with keys in the ignition
- computer with unpatched OS, old browser version, etc.
- dating profile highlighting wealth and loneliness

Operated to find out more information about them (IP address, location, etc.) or provide enough evidence to report

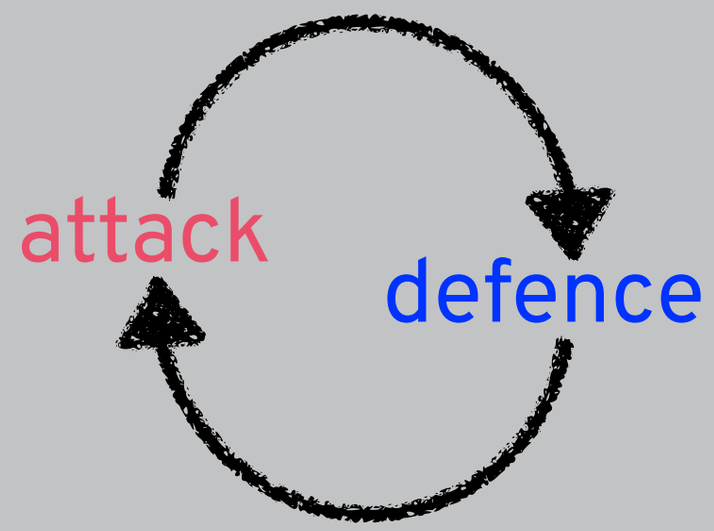
DETECTING ADVANCED FEE FRAUD

This can be even harder than for dating scams because:

- it happens over email (easier to impersonate)
- the target is a willing participant
- scam interactions are designed to resemble normal ones

Still, we can try to look for:

- spam-like distribution patterns
- similar language to known bad emails



REAL ESTATE / RENTAL

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

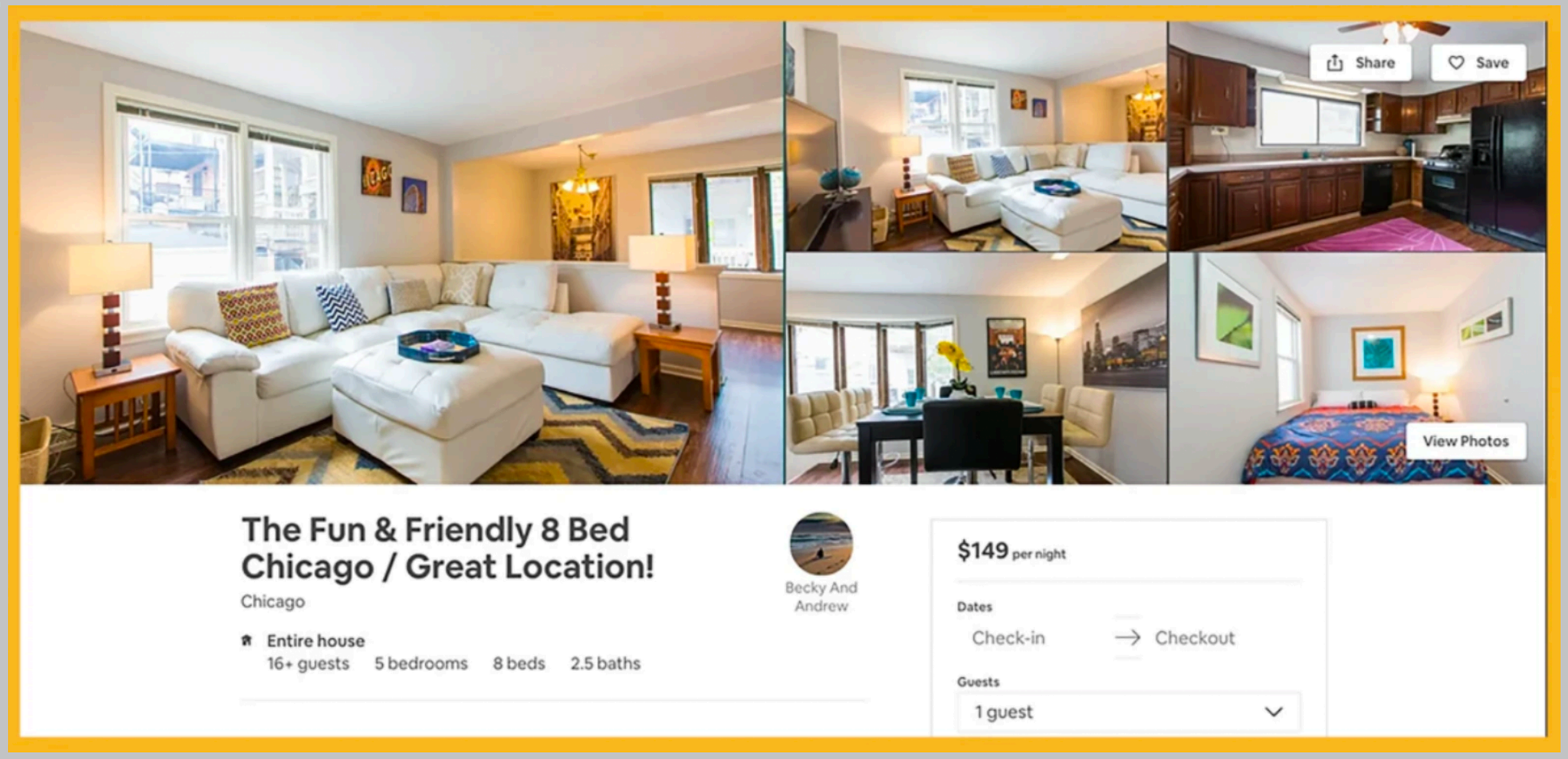
LAST-MINUTE CHANGES

“Sorry, Bob! There were plumbing issues and your rental isn’t available. I have another property but you’ll have to decide right now.”

“...okay I’ll take it.”

<officially change reservation>

PROMISE VS. REALITY



“The whole place felt grimy, and there was a hole punched in a wall. The only decor was a giant wooden cross and a few pieces of generic Chicago-themed artwork, and the dining room's Overstock.com barstools looked as if they would turn into dust if you sat on them.”

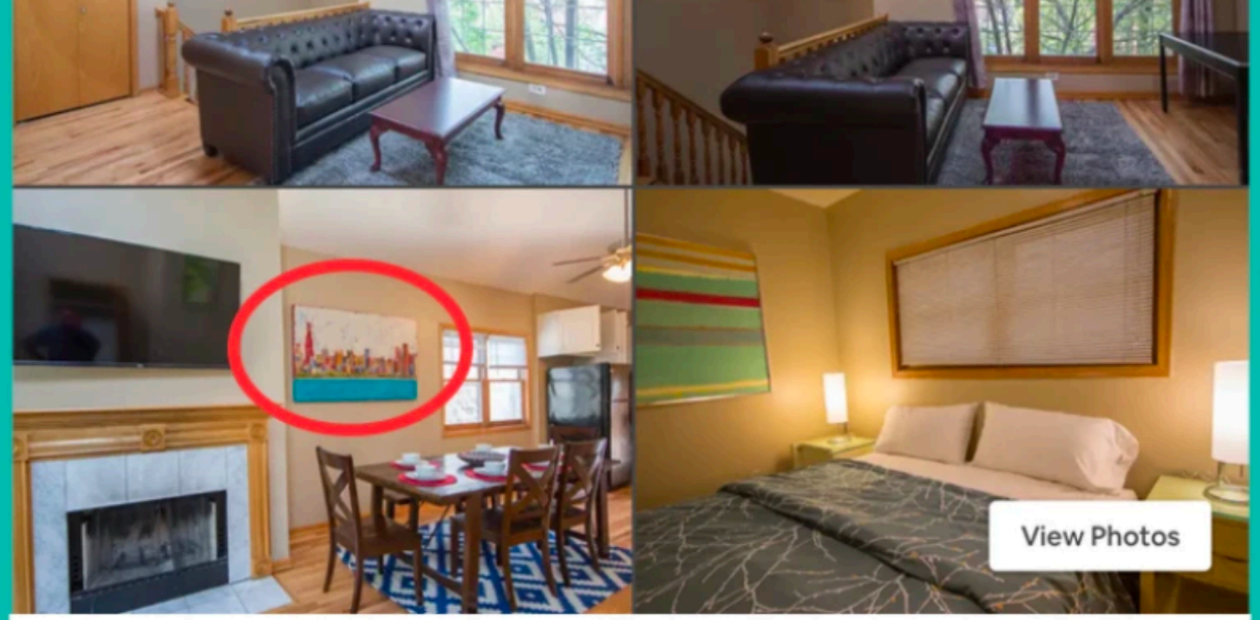
DETECTING SCAM RENTALS

This can be hard because:

- targets don't want to spend time/energy on this
- targets are in a vulnerable position (foreign city, etc.)
- the platform is not really incentivised to address the issue

We can try to look for:

- similarities across listings (need platform to do this)
- bad reviews (positive reviews can be faked)

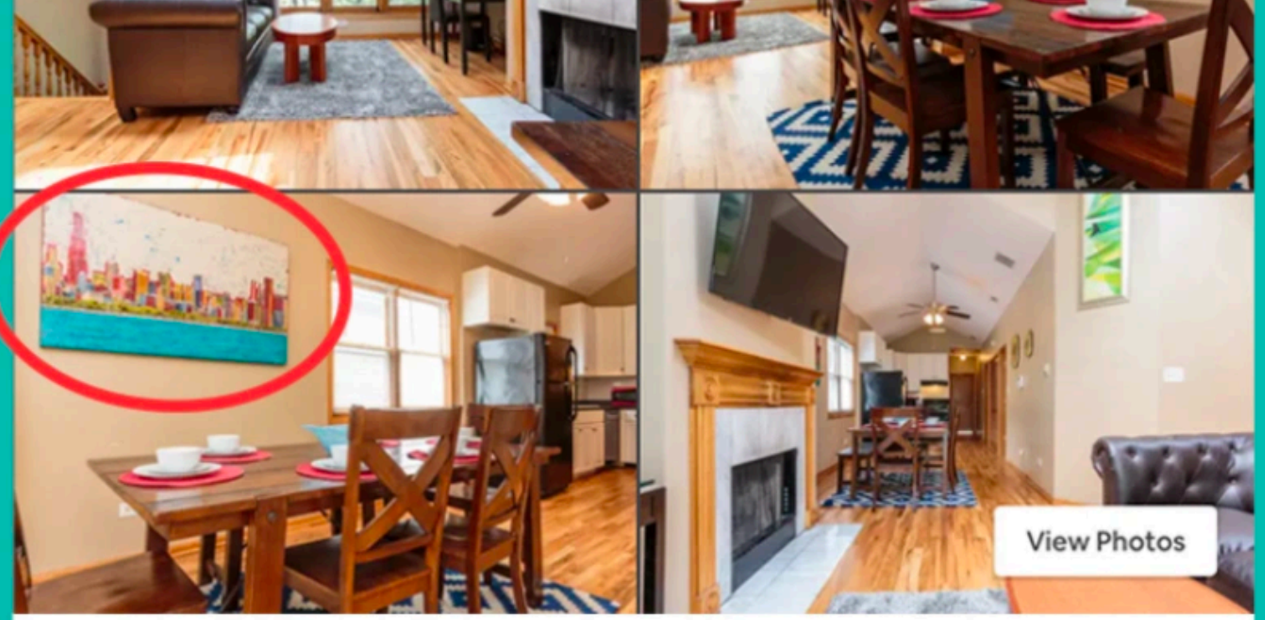


Kris And Becky

$248 per night

Dates

Check-in → Checkout



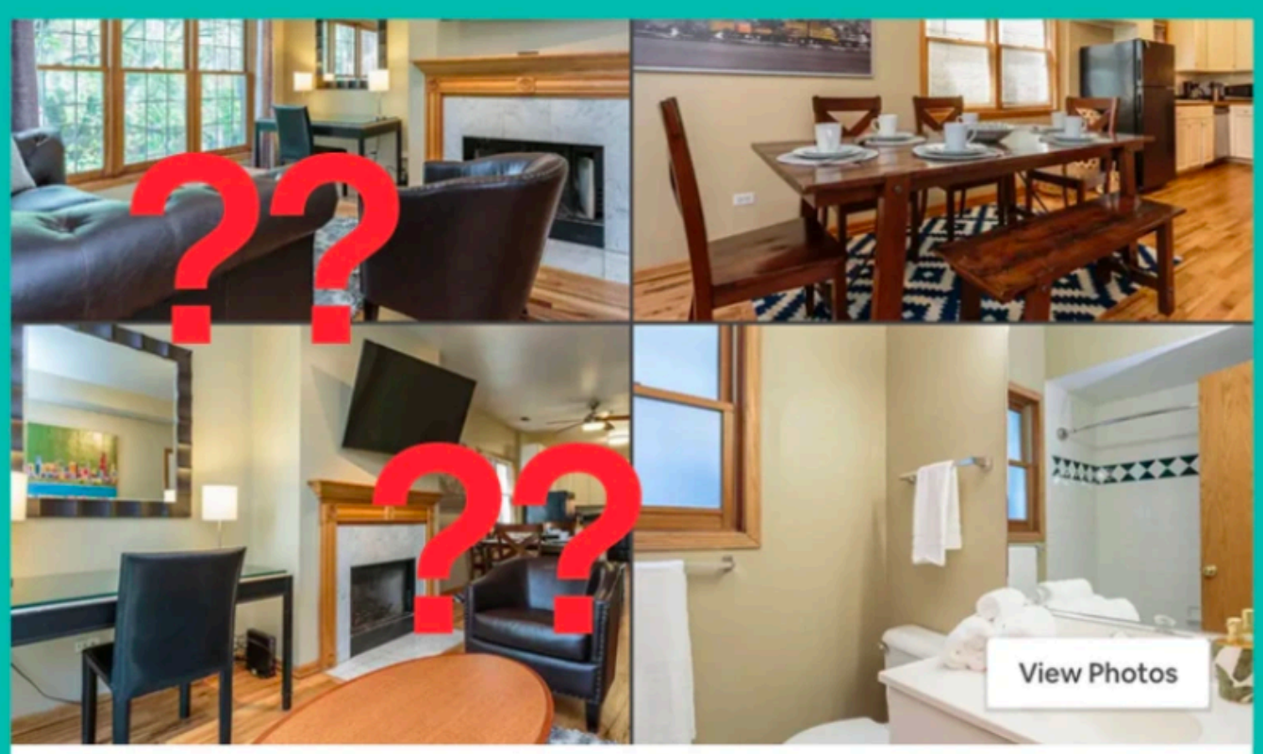
Kelsey And Jean

$90 per night

★4.36 (34 reviews)

Dates

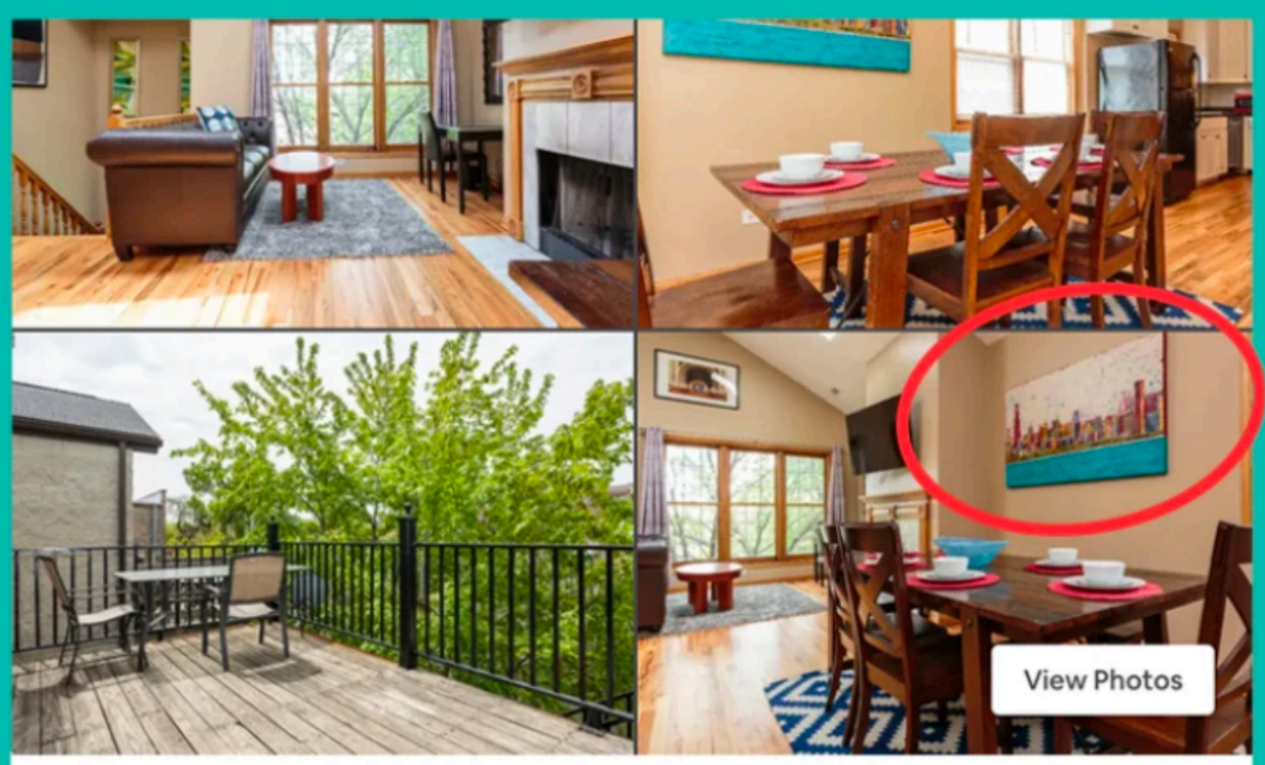
Check-in → Checkout



Alex And Brittany

$119 per night

Dates



Becky And Andrew

$95 per night

Dates

HOW TO IMPROVE

Users lack intuition about complex computing devices →
Provide security education and training

Users are in charge of their own (complex) devices →
Make security invisible

It is hard to estimate risks →
Help users build more accurate mental models

Security measures feel like they get in the way →
Make security the path of least resistance

QUIZ!

Please go to

`https://moodle.ucl.ac.uk/mod/quiz/view.php?id=2778274`

to take this week's quiz!