



Cybersecurity: Fortify Your Business with People, Processes, and Technology


Today's Speaker



Jewel Quintyne
Professional Services Manager
Qualia

Agenda

The Cybersecurity Landscape	04
Current Trends in Cyber Attacks	12
Risks of Not Being Proactive	22
Fortify Your Business with People, Process, & Technology	28
The Value of Cyber Insurance	40



The Cybersecurity Landscape

Why Closings Are An Attractive Target for Bad Actors

Large Sums of Money

Real estate transactions often involve the exchange of hundreds of thousands of dollars

Sensitive Information

Closings require the exchange of large amounts of nonpublic information (NPI)

Reliance on Email

Despite its vulnerabilities, email remains a primary method of communication



Multiple Parties Involved

A typical real estate transaction requires coordination of over a dozen parties

Inexperienced Homebuyers

Buyers are unfamiliar with the closing process and don't know what to look out for

Eager Buyers

Buyers who are eager to finalize the deal may overlook important warning signs

\$173MM

Adjusted losses due to
cybercrime in the real
estate industry in 2023

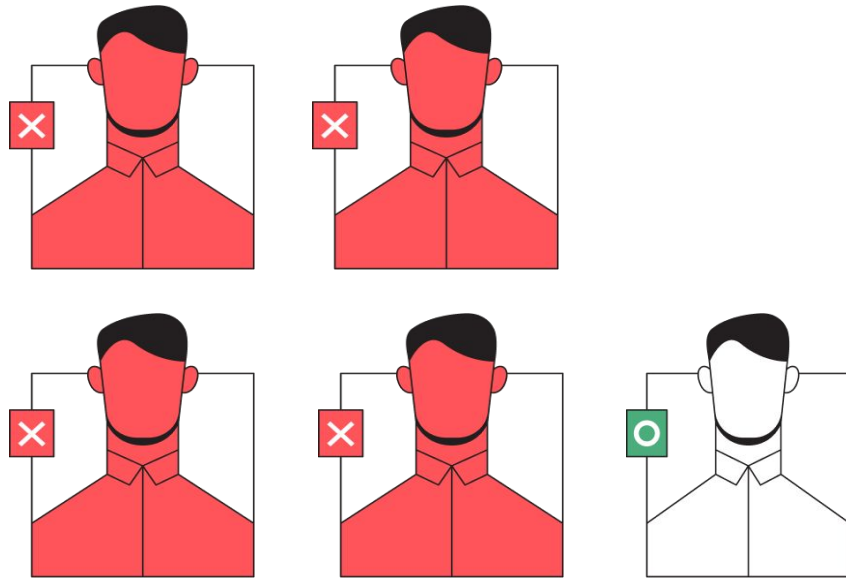
\$143K

Average title insurance
claim cost for fraud and
forgery, according to ALTA

Increase in
losses over
\$50k since
2023



31%



Only 1 in 5
title & escrow
professionals
were able to
recover all funds

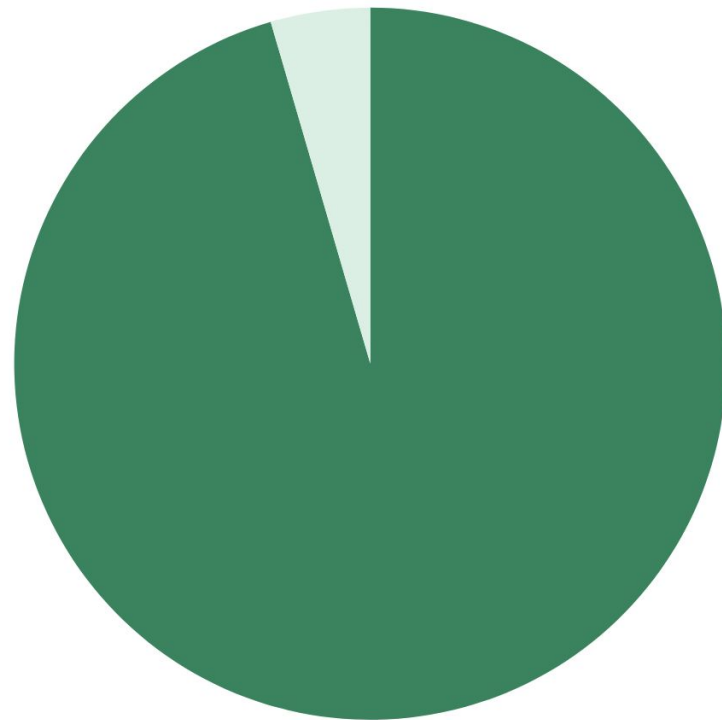
Poll:

How often has your business
experienced wire fraud attempts
in the past 12 months?

The frequency of attacks isn't slowing down

Wire fraud attempts on my business have decreased

4.5%



95.5% Wire fraud attempts on my business have increased or stayed the same

Select the statement which you most agree about the frequency of cyber security attacks on your business in the last 12 months.

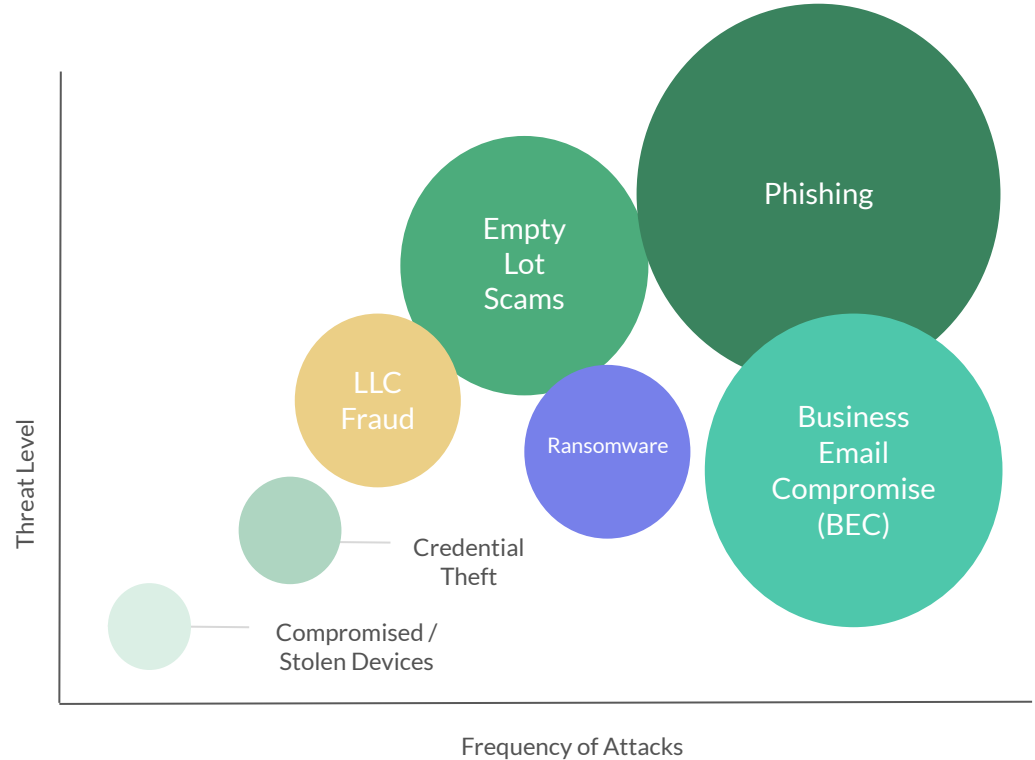


Current Trends in Cyber Attacks

Fraud is becoming more complex and multilayered

Survey Question

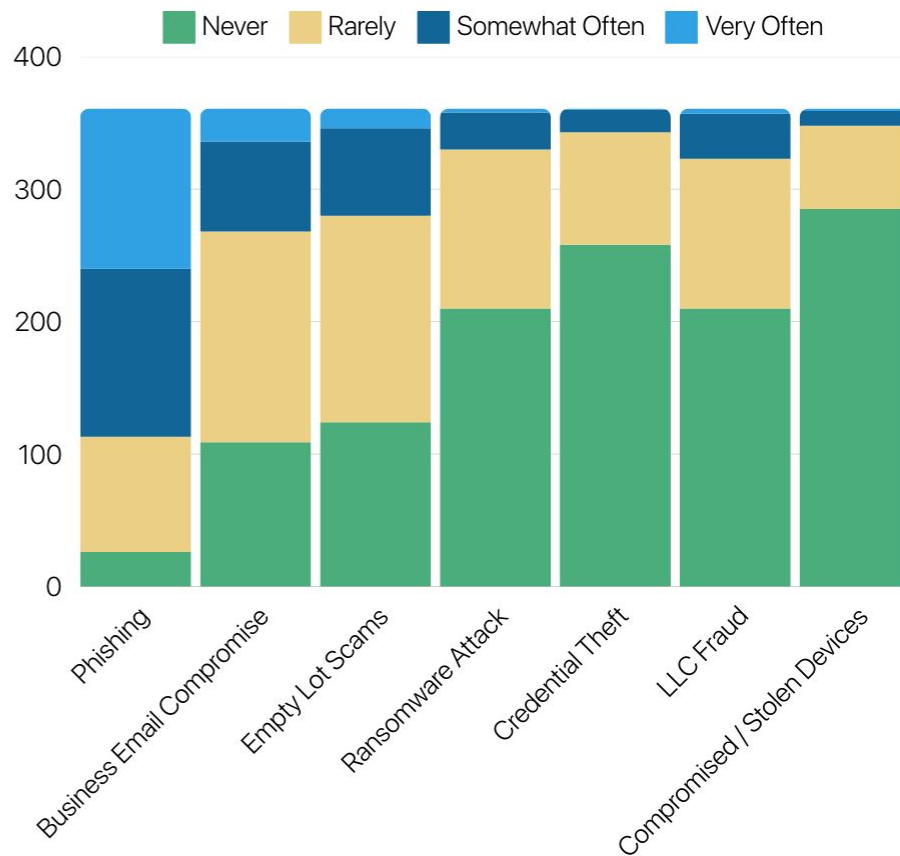
How often has your business experienced these types of cyberattacks in the past 12 months?



Email-based attacks exceed all other trends

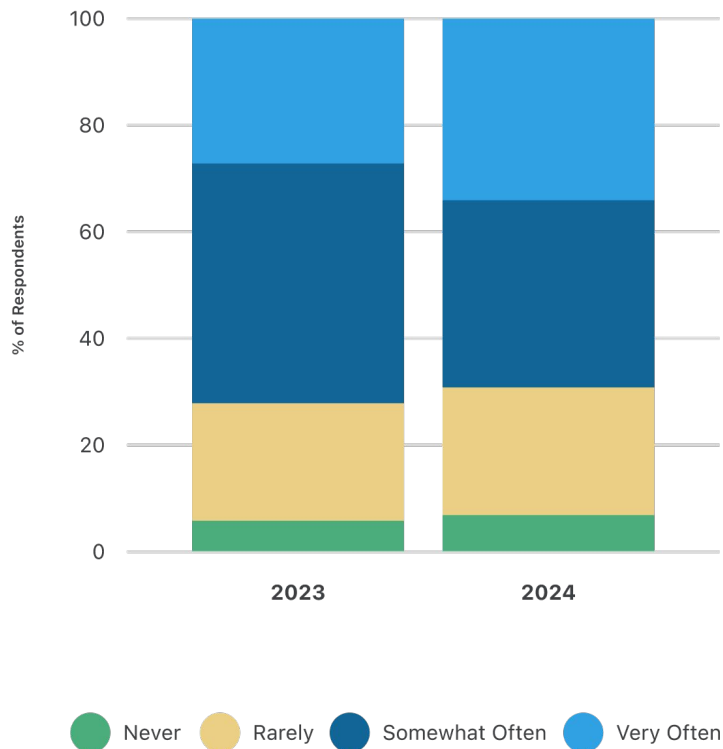
Survey Question

How often has your business experienced these types of cyberattacks in the past 12 months?



Survey Question

How often has your business experienced these types of cyberattacks in the past 12 months?

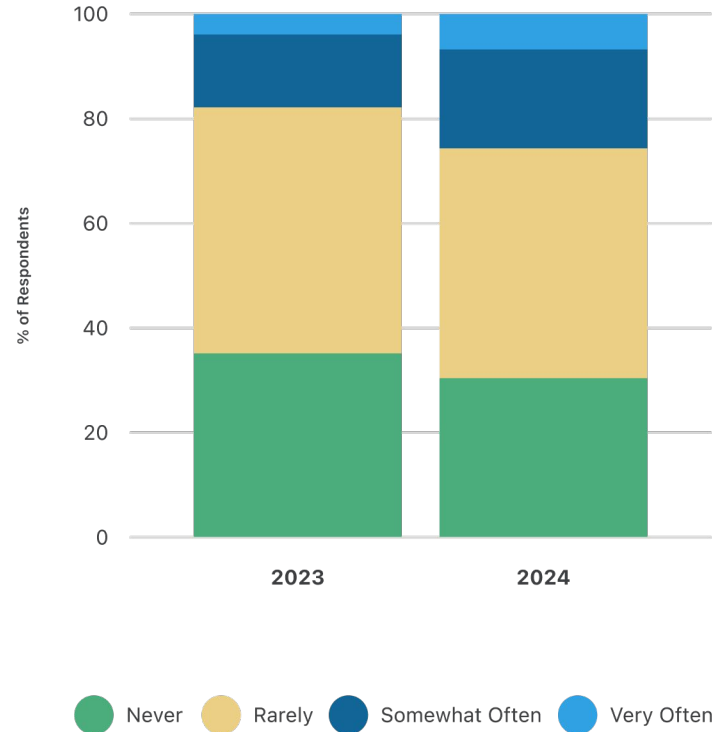


Phishing – the most common type of cyber attack

Business Email Compromise (BEC) is on the rise

Survey Question

How often has your business experienced BEC in the past 12 months?



Survey Question

How often has your business experienced empty lot scams in the past 12 months?

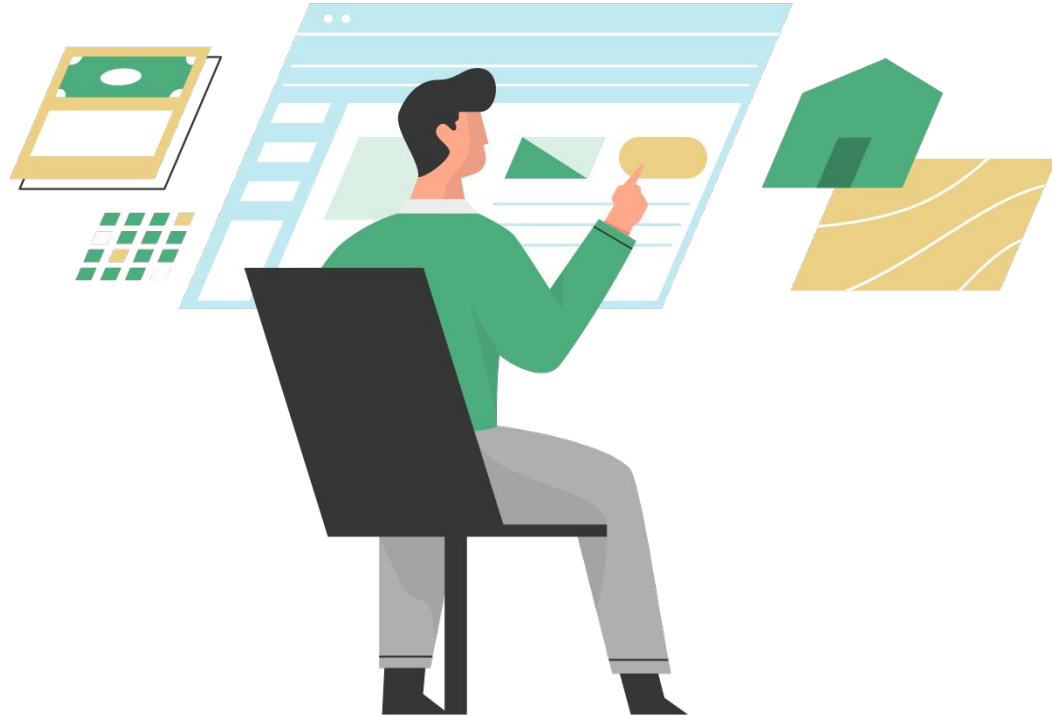


Empty lot scams are increasing

Real Life Fraud

A sophisticated BEC scheme targeted real estate transactions.

Over 400 victims across the United States lost nearly \$20 million.



Real Life Fraud

A woman in Louisiana is fighting to reclaim land that's been in her family for centuries after bad actors impersonated her using a phony ID.

While the buyer's funds were recovered, title for the property has not been restored to the real owner.

Tips to Combat Empty Lot Scams

Verify taxes

Send a certified letter

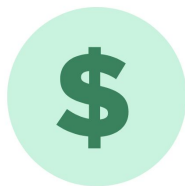
Control the notary

Check public records

Use an ID verification tool



Emerging Threats: Cyber Extortion and Ransomware



Cyber extortion is when bad actors use computer-based threats to coerce victims into giving up money or sensitive data.



Ransomware is a form of malware that encrypts data on a device, making it inaccessible unless the victim pays the attacker a ransom.



A deepfake is a type of synthetic media that uses artificial intelligence (AI) and deep learning techniques to create highly-realistic but entirely fabricated content, including text, audio, images, and video.

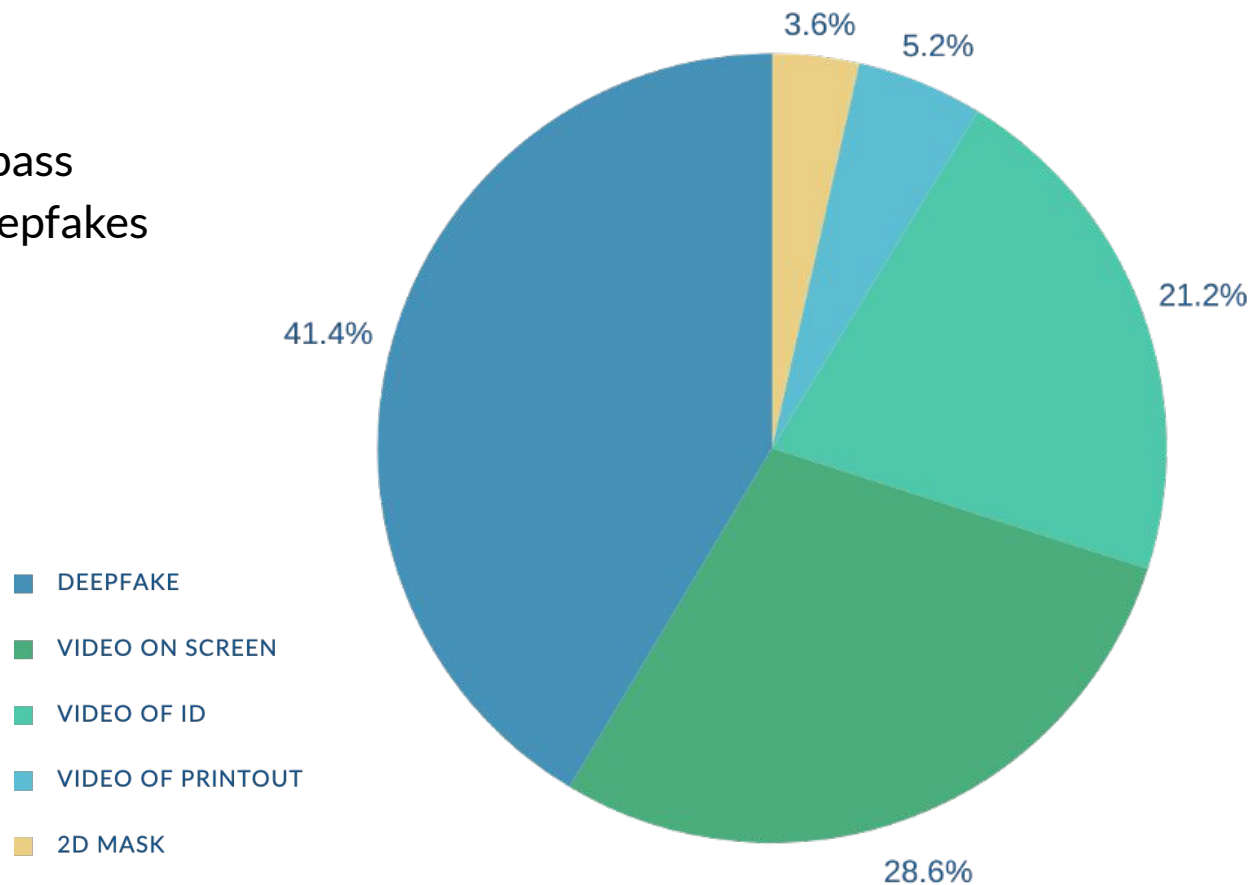
A deepfake attempt
occurred once every
5 minutes in 2024

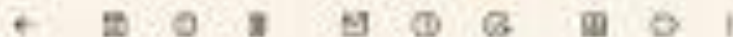
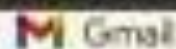
Increase in
deepfakes
since 2022



3000%

Fraudsters use several techniques to try and bypass biometric checks, and deepfakes are the most prominent.





32 of 116



Mike Haze mikehaze@gmail.com

to me

Hey Charlotte,

I've been following the way Qualla is revolutionizing the real estate transaction space, and it's clear you're at the forefront of melding tech with traditional industries. Given your background in Contemplative Neuroscience, I'm curious how you reconcile the rapid tech advancement with the slower, more introspective insights from your studies. **Do you think the relentless push for innovation in tech undermines the value of contemplation and mindfulness that your academic background champions?**

Best,

Mike Haze

cc

Mike Haze

How to Spot Deepfakes

Inconsistent background or environment



Change of skin tone near the edge of the face



Unnatural blinking or eye movements



Unusual delays



Relevancy of speech



Varying tone / inflection



Behavioral Signs of Deepfakes

Avoiding live
interactions



Delaying / denying
additional verification



Overly-scripted
conversations



Conflicting time zone
information



Geographic
inconsistencies



If you suspect a deepfake...



Pause the transaction immediately



Request a second communication channel



Alert your internal fraud team



Notify the authorities

Poll:

Was your business impacted by
any of these fraud trends in the
last 12 months?



Risks of Not Being Proactive

What's at stake?



Monetary loss



Reputational damage



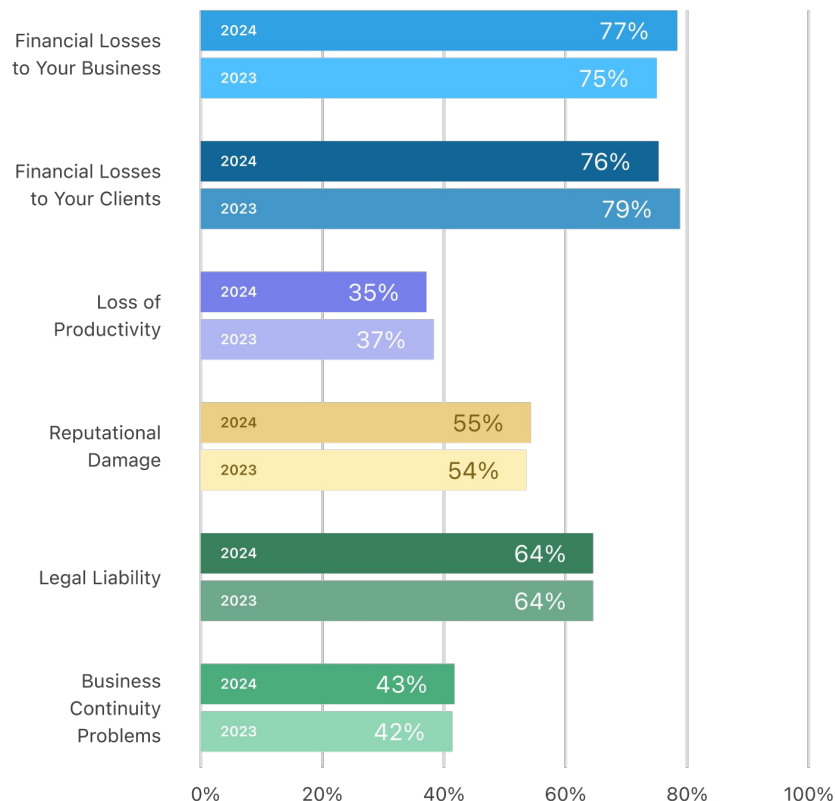
Loss of business


Financial loss remains the top concern

Survey Question

Which potential impact of wire fraud most concerns you?

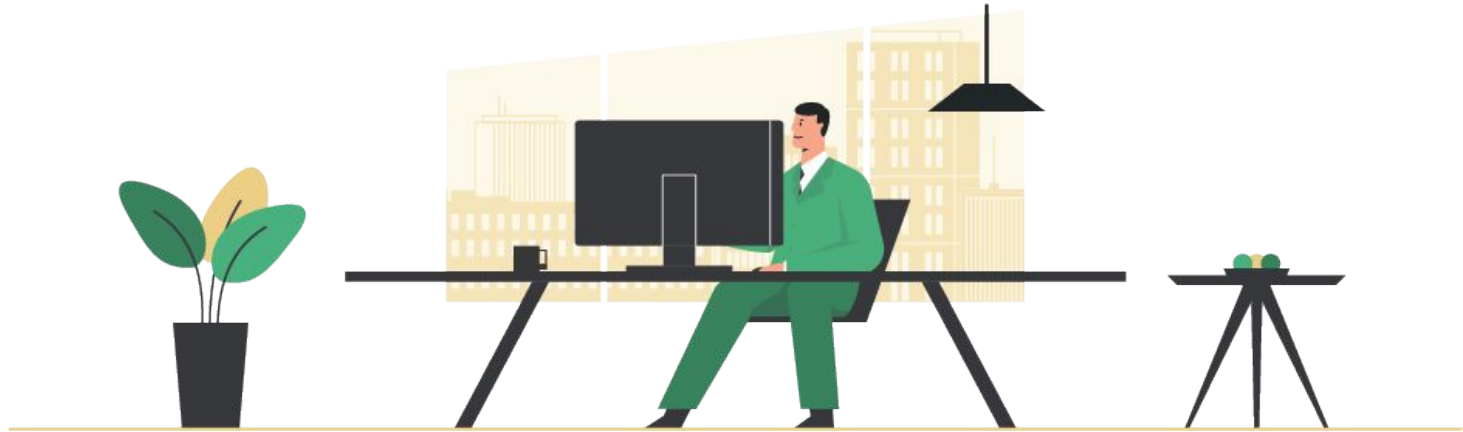
Rank the answers in order from most concerning (1) to least concerning (6).



The background is a solid light beige color. It features decorative wavy lines in a slightly darker shade of beige. One wavy line runs horizontally across the top, with three white dots placed on it. Another wavy line runs horizontally across the bottom, with two white dots placed on it. The text is centered on the left side of the slide.

Fortify Your Business with People, Process, and Technology

A Multilayered Approach to Security Helps Keep Your Business Safe



People —> Process —> Technology



People

Create a **culture of security** within your organization.



Process

Appoint a Security Officer

Make it one person's explicit responsibility to regularly assess the business' security practices against best practices.



Technology

Train and retrain staff regularly

Due to rapid evolution in fraud vectors, security training should be part of regular employee trainings.



People



Process



Technology

Guide all transaction parties to **operate securely.**

- Don't assume cybersecurity is top of mind for everyone.
- Embed education into your transaction processes.
- Make it easy for buyers to act securely.



People —————> **Process** —————> Technology



People



Process



Technology

Embed security into **your processes.**

- Maintain a Written Information Security Plan (WISP).
- Build security best practices into your workflows.
- Periodically review system login activity.
- Keep systems up-to-date.



People —————> Process —————> Technology

Implement password best practices to keep your company secure



Use unique passwords



Use long passwords



Design phrases



Use a password manager

Defend your business with advanced security features



Allowed
IPs



Role-based
access controls



Multi-factor
authentication

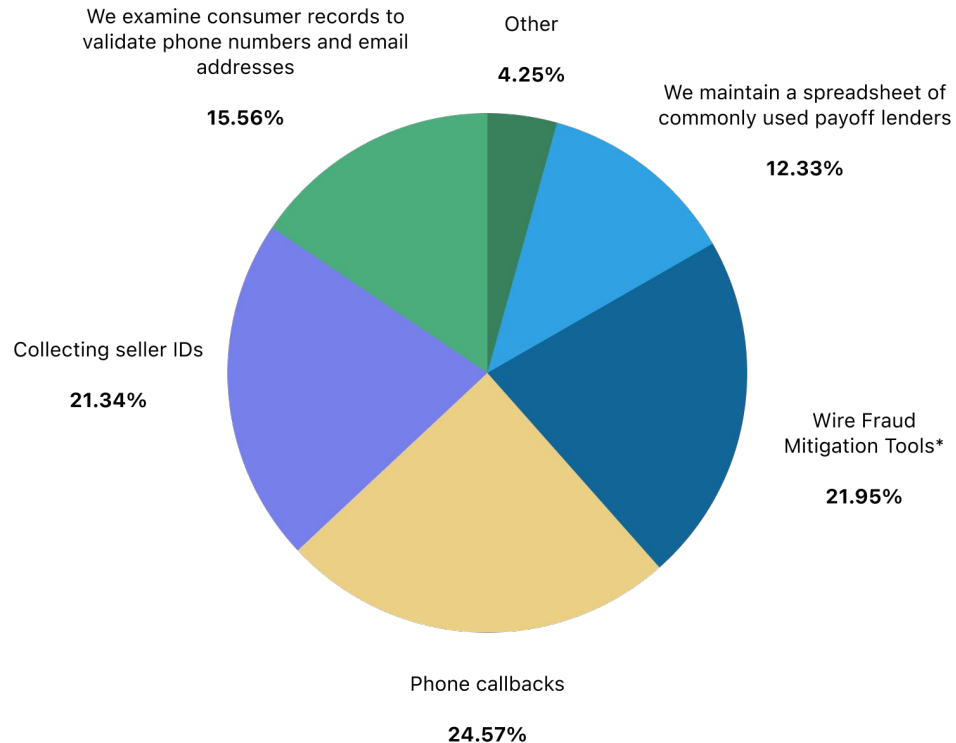


Single
Sign-on

Heavy reliance on manual prevention continues

Survey Question

Which tools or tactics for wire fraud prevention do you utilize? Select all that apply.



*Includes Qualia Connect and Qualia Shield

Employ the Latest Technology to Stop Bad Actors in Their Tracks

Communicate in secure channels

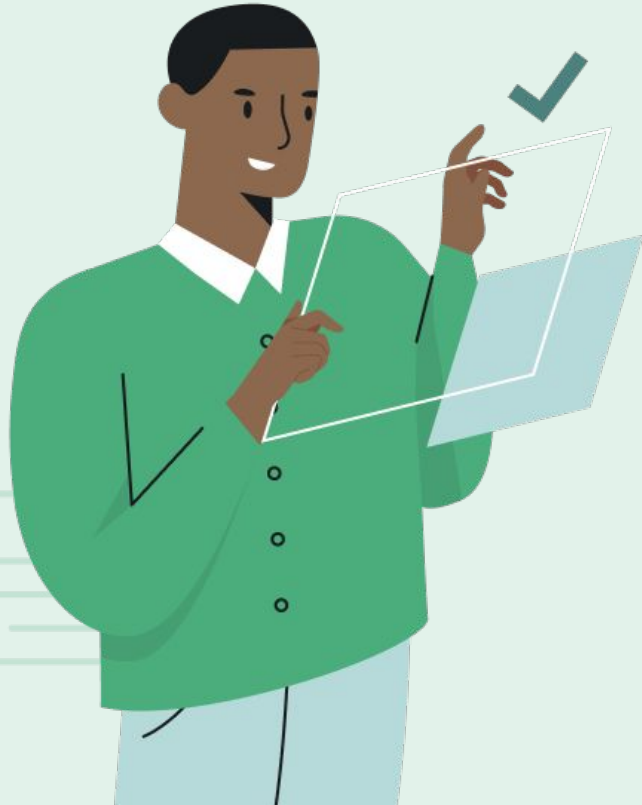
Stop BEC and social engineering, which account for most wire fraud.

Adopt a wire fraud detection solution

Confirm the identity of transaction parties and ensure funds are disbursed to the right person.



How to vet your vendors' security



- ✓ Confirm they adhere to ISO 27001 standards and have gone through SOC 2 auditing
- ✓ Ask for evidence of their ISO 27001 certification and a copy of their SOC 2 report
- ✓ Carefully review their SOC 2 report to see if the auditor highlighted any vulnerabilities, deficiencies, or 'exceptions'

2025 SPECIAL REPORT:

Real Estate Wire Fraud Trends





Thank you!