

Behind the Screen: Defending Against Online Fraud



Questions?

To interact with us
during the webinar,
please use the Zoom
Q&A feature

Welcome!

Please make yourself comfortable, the session will start shortly.



INTRODUCTION



Jeff Brown

Regional Vice President,
Western Canada

PANELIST



Twane Boettinger

Director, Information
Security and IT Risk
FCT



Hilary Palmer

Senior Vice President,
Canada Cyber Practice
Marsh Specialty



Josh Wyatt

Vice President,
Offensive Security
Cyderes

Agenda

- Electronic/Wire Fraud
- Business Email Compromise & Wire Fraud
- Lookalike Domains & Impersonation Fraud
- Cyber Risk – Claims and risk environment
- Q&A

Electronic/Wire Fraud

Understanding the Latest Scams & How to Protect Yourself

What is Electronic/Wire Fraud in Real Estate?

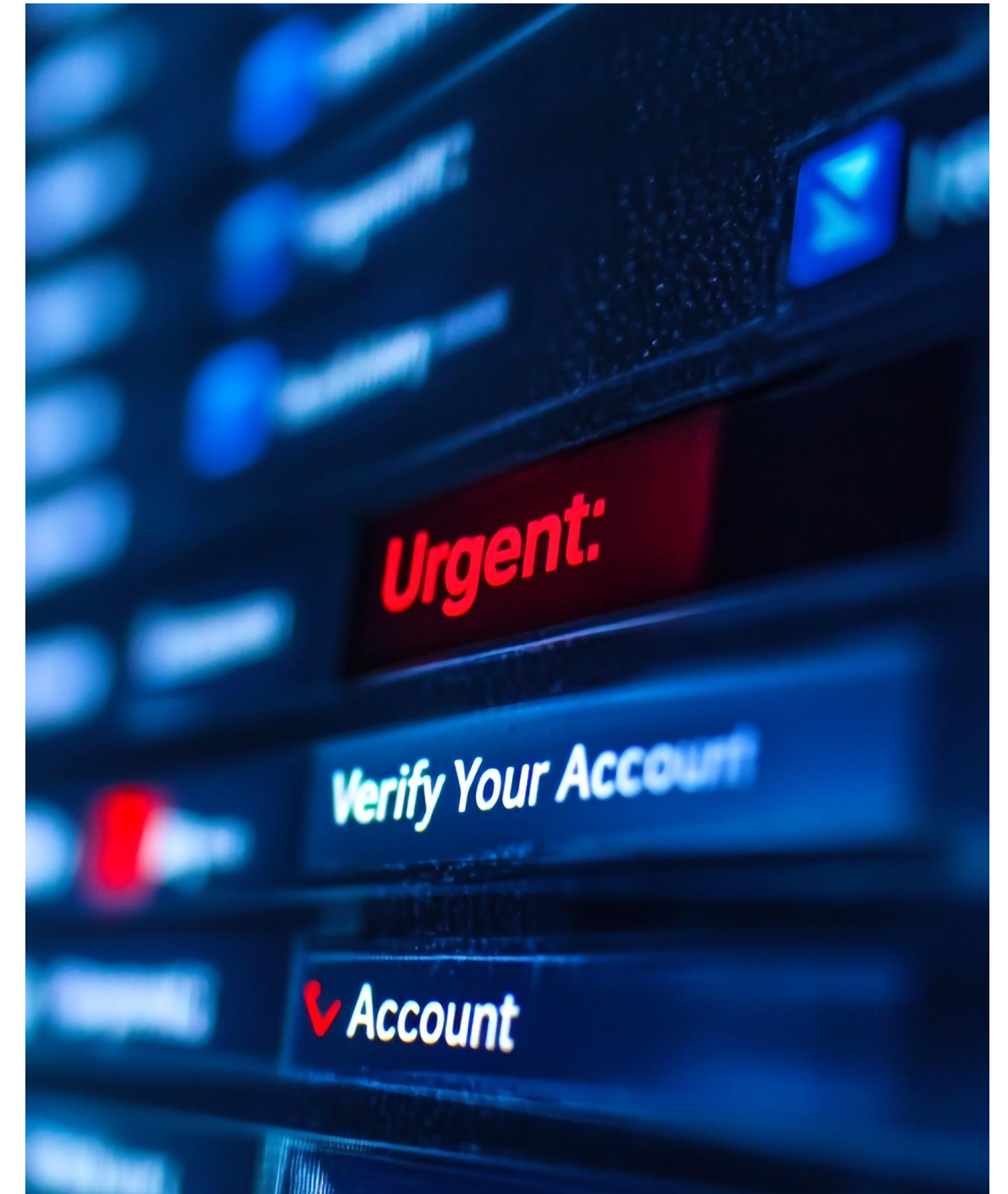
- Cybercriminals exploit technology to manipulate real estate transactions.
- Financial losses can be significant, impacting buyers, sellers, and professionals.
- Increased sophistication of scams with AI and deepfake technology.



Business Email Compromise (BEC) & Wire Fraud

How It Works:

- Scammers **infiltrate email chains** and impersonate parties within the real estate transaction.
- Continue to use the legitimate email account of a party but **hide their tracks** so the owner of the account is not alerted.
- Ultimate goal is to provide **fraudulent wiring instructions** to trick victims into transferring funds.



Business Email Compromise (BEC) & Wire Fraud


THE U.S. Sun News Sport TV Entertainment Money Tech Motors Travel Lifestyle More

Money > News Money

CLOSING COST Woman's 'whole world fell apart' after \$255K savings vanished in huge housing scheme – single email took everything

Plus, an expert's breakdown of what to look out for

Jacob Willeford, Consumer Reporter
Published: 17:58 ET, Mar 3 2025 | Updated: 17:58 ET, Mar 3 2025



HOUSING SCAM

- Victim received an email she thought was from her title company.
- The email provided instructions on how to wire the money for closing.

Business Email Compromise (BEC) & Wire Fraud

Pro Prevention Tips



Always verify wire transfer details via a trusted phone number or previously confirmed method.



Be suspicious of last-minute changes in wiring instructions.

Lookalike Domains & Impersonation Fraud

- Similar to BEC however the bad actor creates domains that closely resemble legitimate firms.

Original Domain **example.com**

Using Digit "1" **example.com**

Using Cyrillic "ë" **ëxample.com**

Using Cyrillic "a" **example.com**

Lookalike Domains & Impersonation Fraud

- These **fake domains** are used to establish websites and email addresses to trick victims into engaging with fraudulent actors thinking they are the legitimate parties.
- This is often tied to a successful BEC attack which is first used to identify an emerging real estate deal and then **hijack the email thread** by inserting lookalike domain addresses and removing the authentic recipients.

amazon.com



www.amazOn.com



www.amazon-store.com

Lookalike Domains & Impersonation Fraud

Pro Prevention Tips



Enable browser control to check for typo domains
- do not rely on this alone!



Double-check email addresses for slight misspellings or extra characters.



Verify website URLs before entering sensitive information.



Always confirm wire instructions verbally using a known phone number.

Given these 4 domains, which ones do you think is the intended domain?

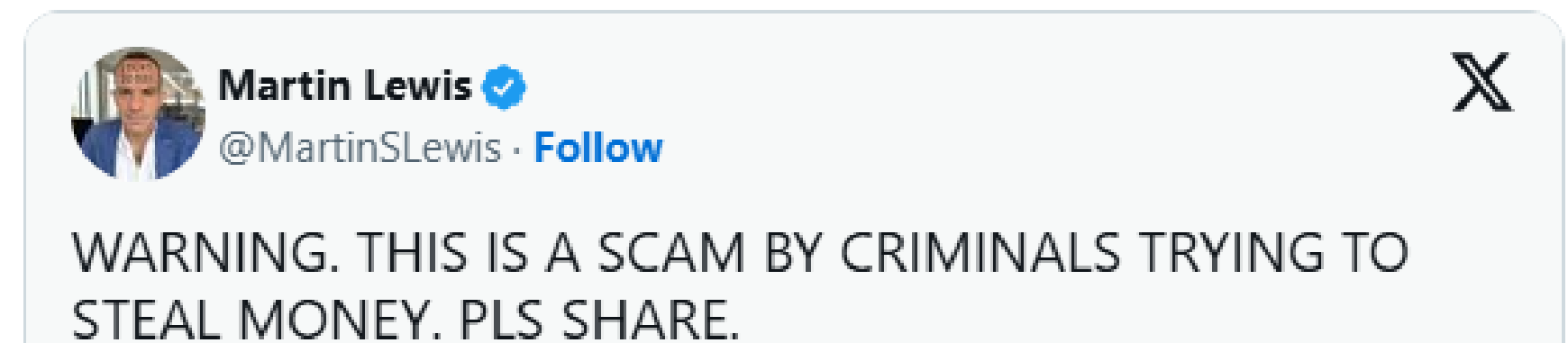


Deepfake Technology in Scams

How It Works:

- Fraudsters use AI-generated fake identities and videos to impersonate trusted parties.

Example: A call center scam in Georgia used deepfakes, including Martin Lewis, to steal \$35 million from 6,000 victims.

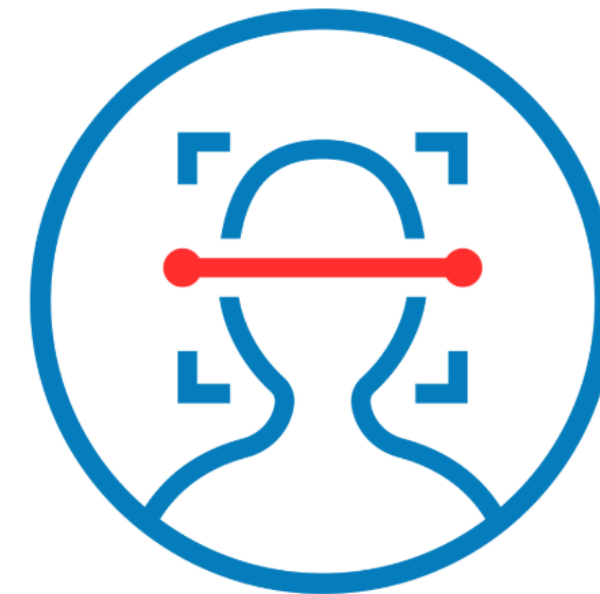


Deepfake Technology in Scams

Pro Prevention Tips



Be wary of suspicious video calls or documents that look manipulated.



Use biometric verification or in-person meetings for critical transactions.

Key Prevention Strategies

- **Be Cautious:** Approach transactions with healthy suspicion. Think twice before acting. Pay attention to warning signs.
- **Verify Communications:** Double-check emails and calls before sending funds. Use previously proven or out-of-band methods to validate authenticity.
- **Enable Multi Factor Authentication everywhere:** While MFA significantly reduces the risk of unauthorized access, no security measure is foolproof. Stay vigilant, use strong, unique passwords, and be aware of phishing or MFA-bypass attacks.



What to Do If You're a Victim of Electronic/Wire Fraud

- **Contact the Bank(s) Immediately** – Ask them to cancel or attempt a recall of the wire transfer.
- **Report to Authorities** – In Canada, report to the Canadian Anti-Fraud Centre (CAFC), Canadian Centre for Cyber Security and local law enforcement.
- **Notify Parties in the Transaction** – Inform other legal professionals, real estate agents, and title company.



Canadian Centre for Cyber Security
www.cyber.gc.ca/en

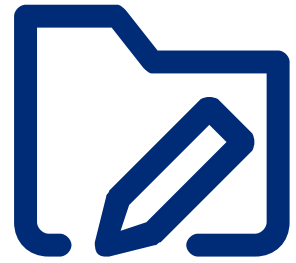
Report a cyber incident

What to Do If You're a Victim of Electronic/Wire Fraud

- **Work with your Cybersecurity Experts** – If your email or device was compromised, take steps to secure your accounts. Change your password and access methods immediately. Update your account recovery methods (security questions for instance).



Cyber Risk – Claims and risk environment



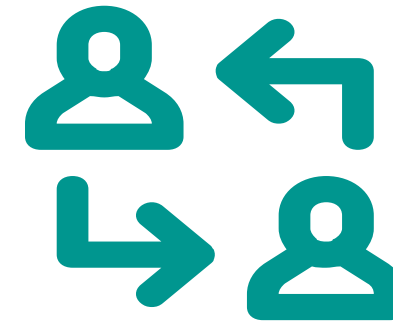
Top 5 Affected Industries

- Professional services firms have been among the top 5 industries in Canada reporting Cyber events



Cyber Events

- Ransomware continues to be a key cyber claim driver
- Phishing attacks are an entry point to larger breaches
- Attackers continue to get more sophisticated
- Number of companies paying the ransom demand is decreasing
- Lateral movement and data exfiltration key tactics for threat actors



Third-Party Cyber Risk

- Third-Party dependency on technology poses additional risk
- Widespread use of technology providers
- Growing interconnectivity between organizations



Privacy & Regulatory

- Claims frequency rising in connection with broader privacy regulations & rights
- Personal Health Information Protection Act- Ontario
- Quebec's Private Sector Privacy Act
- Amendments in Canadian landscape align with global legislation and guidelines

Accreditation information

Legal Professionals

- **British Columbia**
Qualifies for **1 hour** of CPD credit with the **Law Society of B.C.**
Qualifies for **1 CE credit** with the **Society of Notaries Public of B.C.**
- **Ontario**
This program contains **1 hour** of **Professionalism Content**.
- **Rest of Canada**
Please check with your local governing body to determine qualification for credit.

Mortgage Professionals

- Pre-approved by Mortgage Professionals Canada for **1 CE Unit in the Compulsory category**.

The session recording and a copy of this presentation will be available **FCT.ca** in the next few days.

Thank you!

www.fct.ca/webinars

