Cybersecurity for Estate Agents

Why Estate Agents Are Targeted

- Estate agents are involved with large financial transaction amounts and the handling of sensitive identifying information and deposit funds, as well as providing mortgage and other financial details. These transactions typically involve a high level of client trust and high urgency to complete. The increase in hybrid working and branch access is making estate agents more exposed to criminals. The majority of cyber attacks against estate agents are not technical hearings. These are attacks based on email.
- From an estate agent's perspective, security means safeguarding your client's trust in you as an agent so that you can continue to gain new business.
- **Tone:** Calm, professional, without causing hysteria.

The Biggest Cyber Risks Facing UK Estate Agents

These risks are presented in a manner to provide a simple and pragmatic overview of the top 10 risks associated with these types of attacks:

1. BEC (Business Email Compromise)
2. Redirected Funds Invoice/Payment Fraud
3. Phishing Targeting Negotiators and Branch Staff
4. Common Passwords Used for Multiple Portal Log-Ins
5. Shared Inbox Access (sales@, lettings@)
6. Unsecure Remote Working
7. Mobile & Laptop Theft/Loss
8. Exposure to CRM/Property Platforms
9. Use of Public Wi-Fi During Viewings/Travel
10. Compromise by Third Parties (Solicitors, referencing agents).

The 10 risks presented above are prevalent in the way in which estate agents operate in the UK, including the offer process, coordination of the exchange of the offer, discussions with the client about paying the deposit, anti-money laundering checks, etc.

How Property Transaction Fraud Works (Step-by-Step Explanation)

A clear and concise narrative outlining how Crooks gain access to property transactions.

PHASE 1: Initial Access

- Phishing e-mail.
- Password reuse.
- Stolen credentials from data breaches.
- Access to a Solicitor's account.

PHASE 2: Silent Monitoring

- Invoicing rule creation.
- Tracking transaction communications.
- Identifying settlement dates.
- Learning tone and style of communication involved in the transaction.

PHASE 3: Payment Redirecting

- Fake e-mail “from Solicitor”.
- Change to bank account number.
- Urgent message sent to pay before settlement occurs.
- Slight variation in spelling of domain names.

PHASE 4: Transferring Money

- Money transferred into a mule account.
- Money stripped out quickly.
- Difficult to recover.

NOTE:

- Often appears very legitimate.
- Fraud relies heavily on urgency and trust.

Real-World UK-Style Scenarios

Each example includes:

- What occurred
- How the intruder gained access
- Indicators of danger that were not noticed
- Financial and reputation impact
- What could have stopped this from occurring

Example 1: Criminal Impersonating Lawyer During Exchange

- Fake domain email.
- Redirecting the deposit.
- Prevention: verification call system, MFA, impersonation protection.

Example 2: Hacked Account Compromises Payment Details in Microsoft 365

- Compromised negotiator account.
- Hidden inbox rules.
- Changed instructions for payment.
- Prevention: MFA, conditional access, monitoring.

Example 3: Negotiator Clicked Link to "Property Portal" Phishing Email

- Thief collected user credentials via fake login website.
- Thief used credentials on other sites.
- Accessed CRM.
- Prevention: training on phishing and use of MFA.

Example 4: Staff Sent Contracts Using Gmail, Personal Account

- Impossible to track emails.
- Account was subsequently compromised.
- Data was compromised.
- Prevention: secure sharing platform for documents; non-negotiable.

Example 5: Buyer Identification Provided for Stolen Laptop

- Stolen laptop from trunk of car.
- No encryption on files.
- Stored Anti-money laundering documentation on local hard disk.

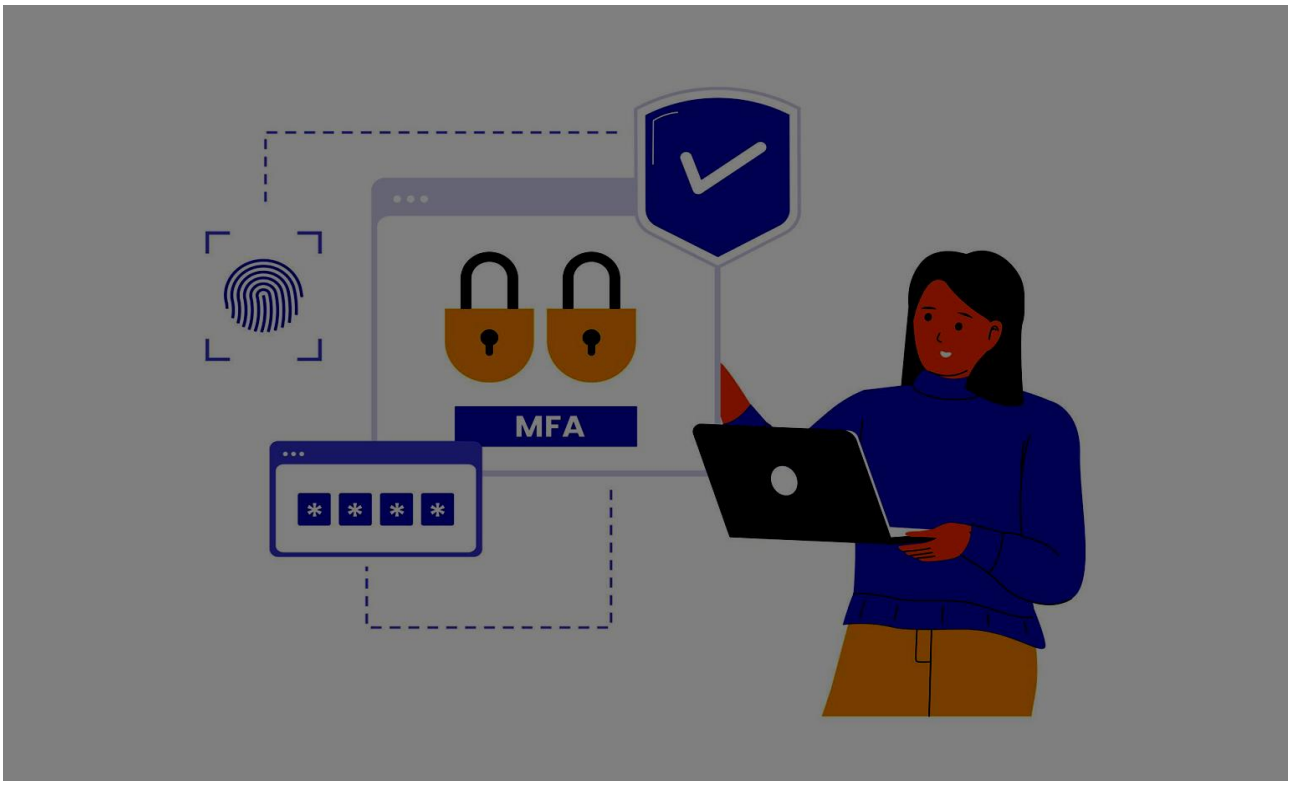
Prevention: full disk encryption, use of cloud storage for documents, ability to kill an encrypted disk.

Security Controls Every Estate Agent Should Implement

This section is arranged by their level of importance.

1. Multi-Factor Authentication (MFA)

- MFA is a requirement for all Microsoft 365 accounts, CRMs and portals.
- Reasons that explain why password only authentication fails.
- Two different types of multi-factor authentication, SMS and app-based, each have their advantages/disadvantages.



2. Conditional Access

- Block access for high-risk logins.
- Block access for anyone logging in from a geographically identified high-risk country.
- Only allow access with compliant devices.

3. Email Filtering and Impersonation Protection

- Anti-spoofing measures (e.g. SPF, DKIM, DMARC) are very important.
- Detection of impersonation attempts.
- Safe Links/Safe Attachments.

4. Secure Document Sharing

- Do not send any ID documents via email.
- Use only encrypted portals to send documentation.
- Enforce the use of expiring links for all documentation sent out.

5. Endpoint Encryption

- Use BitLocker or another comparable technology.
- Ability to remotely wipe any devices that are lost or stolen.

6. Regular Staff Phishing Awareness Training

- Train your staff on how to recognise phishing. Keep them updated on the latest techniques every few weeks.
- Conduct simulated phishing attacks to test employees knowledge after training.

7. Backup and Ransomware Resilience

- Backup all data to separate and secure locations.
- Regularly conduct test restores of backup data.
- Backup your CRM system.

8. Clear Payment Verification Process

- Obtain mandatory verbal verification of bank account details provided via email or telephone before making any payments to third parties.

9. Joiners and Leavers Controls

- Immediately remove access to systems of employees who leave the company.
- Change passwords of employees who change their roles within the organisation.

Invoice Fraud Prevention and Email Security

Estate agency workflow:

- Always verify bank detail changes with the client by phone.
- Have a banner warning of external email sources.
- Disable auto-forwarding.
- Monitor your inbox rules.
- Have a standard email disclaimer advising about bank details.
- Educate your clients using the following statement 'we will never change our bank details via email alone.'

Explain how to communicate this without making your clients feel alarmed.

Protecting Client ID Documents and AML Data

High-level overview of AML obligations:

- Estate agents must verify the identity of all clients before accepting them as clients and keep records of all clients' personal identification materials.
- This includes but is not limited to passports/driving licences/proof of address.
- The types of documents obtained from your clients are highly sensitive in nature.

How to explain:

- Use secure storage (example: do not store records on local machines at your agency).
- Role-based access to client records.
- Encryption of records.
- Retention periods for all records.
- Deletion policy.
- Your duties under the UK GDPR.

Secure Hybrid and Branch Working

Reflective of Current Agency Structure:

- Multiple locations for offices
- Bridging/Sharing between Team members working from home
- Moving around accessing jobs between viewings

Coverage of:

- Home Wi-Fi security
- Devices that can connect wirelessly to the internet
- VPN vs. Cloud based systems
- Internet risks when using Public Wi-Fi
- Mobile Device protection
- Using workstation/PCs of others colleagues at shared workspaces

Data Breach Response Considerations

High-Level Considerations:

- What constitutes a data breach?
- ICO 72-hour reporting rule.
- Incident documentation.
- Notify affected clients.

- Importance of early containment and mitigation.

Keep the document concise but thorough and accurate.

90-Day Practical Security Improvement Roadmap

Days 0-30: Immediate Risk Reduction

- Enforce multi-factor authentication (MFA).
- Enable data encryption.
- Disable legacy authentication.
- Review access for shared inboxes.
- Draft payment verification policy.

Days 30-60: Consolidating Defence Controls

- Implement email impersonation protection.
- Provide staff with phishing training.
- Implement conditional access policies.
- Complete backup review.

Days 60-90: Building Maturity and Governance

- Create an incident response plan.
- Create or enable joiners/leavers checklists.
- Conduct anti-money laundering data audit.
- Consider Cyber Essentials compliance certification.

Estate Agency Cybersecurity Checklist:

Technical

- Have MFA configured?
- Are devices encrypted?
- Email filtering implemented?
- Are backups tested?
- Conditional access configured?

Procedural

- Is there a Payment Verification Policy?
- Is there a documented leaver process?
- Has an Incident Plan been developed?
- Is there a staff training plan/record?

Data Protection

- Is AML data stored securely?
- Is access controlled?
- Is there a retention policy in place?

FAQs

➢ **Why Are Estate Agents Targets?**

Estate agents engage in significant financial dealings and deal with sensitive information (ID, banking) making it easy for a fraudster to monetise by redirecting funds or stealing identities.

➢ **How Does Payment Redirection Fraud Occur?**

Cybercriminals will compromise a person's email account; they can then insert false banking details during an exchange or completion of a property to divert funds from a deposit before it is detected.

➢ **Is Antivirus Sufficiently Protected?**

Antivirus will assist with malware protection but to protect against fraud and phishing attacks, strong authentication (MFA), education, and verification processes must also be in place.

➢ **Should Bank Details Be Verbalised Over The Phone?**

Yes: all changes should be verified using known phone numbers; email-provided phone numbers should not be used to make this call.

➢ **Do Smaller Independent Agents Face The Same Risk?**

Yes: smaller agents have fewer resources than larger agents but are still targeted; therefore, basic, such as MFA, are easy to institute as a scalable process.

➢ **Will Cyber Essentials Help?**

Yes: the government-approved Cyber Essentials scheme includes basic controls that will reduce insurance premiums and demonstrate compliance with GDPR.

About this guide

The **Computer Support Centre** has created this Security Actions For Estate Agents Guide, which provides simple, practical solutions to help protect the data and systems of estate agents and small businesses from threats. The guide was produced from the National Cyber Security Centre (NCSC) guidance, Property Sector Incidents (PIS) research data, ICO reports and Action Fraud Alerts for 2021-2026, and is designed with busy journalistic/operations in mind, to ensure that all of the information included within it is easy to implement and deliver measurable benefits. The Safety Actions For Estate Agents Guide includes straightforward guides for finance-related security topics including:

- Microsoft 365 security services including Multi-Factor Authentication (MFA), email filtering and conditional access
- Phishing training and simulated phishing exercises

- Secure file sharing and Anti-Money Laundering (AML) document protection
- Payment fraud prevention policies and processes
- Cyber Essentials support and testing
- Quick security audits or reviews

If you are interested in speaking with us about your agency or would like to schedule an informal chat or short checklist review of some of the security concerns affecting your business, please do not hesitate to contact us. We are committed to providing you with simple, effective solutions.

For more information regarding how **Computer Support Centre** can assist with your Cybersecurity for Estate Agents please visit https://computersupportcentre.com.

Conclusion

Cybersecurity is about supporting client trust and providing seamless and secure transactions for UK estate agents. By making simple adjustments, such as enabling MFA, confirming payments via phone, training staff on how to protect themselves against phishing, and lock down your devices and documents from unauthorised access/changes, you will be able to significantly reduce the most significant risk to your agency particularly payment redirect fraud and data breaches without slowing down your business at all.

These practical controls will allow your agency to comply with UK GDPR and AML standards, enhance client trust, and in many cases reduce your cyber insurance premiums. This week, choose one or two items from the checklist to implement, making small changes has a significant impact.