Clear and Present Danger in the Real Estate Industry – Cyber Security Awareness Update

Speaker
Colleen M. Capossela

CATIC
AGENT DRIVEN. INSURING RESULTS.

CATIC PRO INC.
PROFESSIONAL SOLUTIONS FOR YOUR BUSINESS

Overview

Real Estate Industry

Target

All

All impacted regardless of size; All participants!

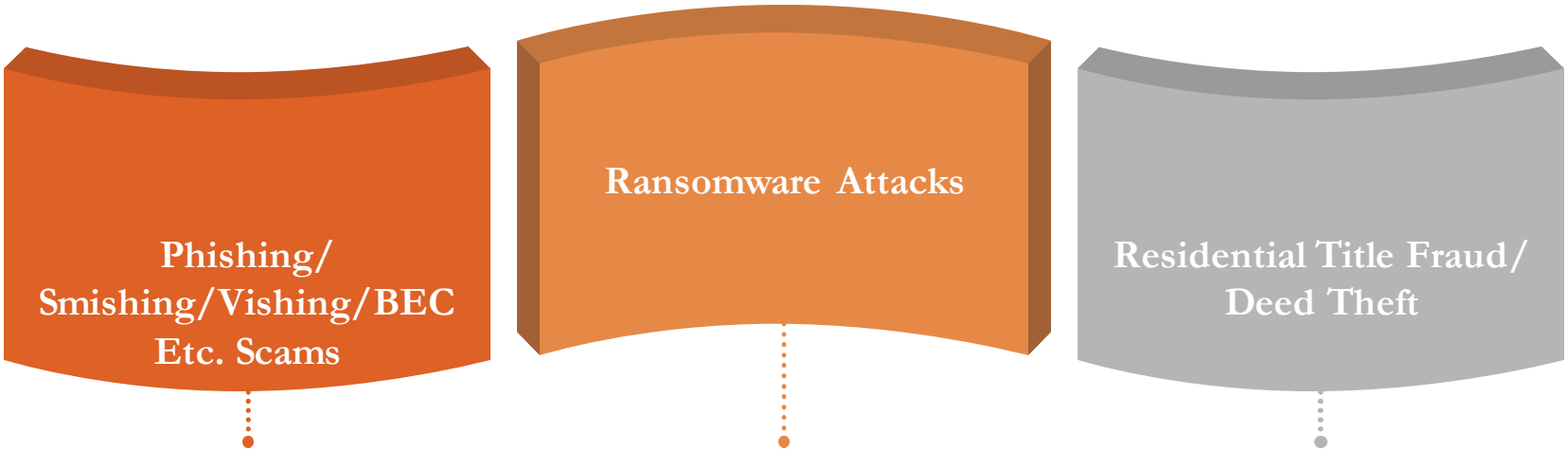
Ever Changing, Ever Evolving!

Risks

Awareness

Educating and Planning is key!

Crimes Affecting the Real Estate Industry – Overview of Certain Areas (Not All-Inclusive) - For example:



Phishing, Smishing, Vishing, etc…

- **Phishing** is a type of social engineering attack usually via email with an attempt to steal data, including, but not limited to, login credentials, account information, credit card numbers etc., or to trick you into opening a malware-laden attachment or clicking on a malicious link, or to dupe you into transferring funds.

- **Smishing** is a combination of "SMS" (short message services, better known as texting) and "phishing." Smishing simply uses text messages instead of email.

- **Vishing** is a combination of "voice" and "phishing." Vishing is generally conducted by phone.

- **Spear-phishing** is a targeted attempt to steal from a specific victim.

- **Whaling** is a highly targeted phishing attack aimed at executives.

- FAX? AND WHAT ABOUT ***PHARMING***

More Details on Phishing

SOME EXAMPLES OF CERTAIN PHISHING EMAIL REQUESTS FROM: Managers/Supervisors to Unsuspecting Employees

In Subject Line:

- *Are you available?*
- *Can you do me a favor?*
- *Request.*
- *Quick Task.*
- *Quick Response.*
- *Confirm if you are available.*

Then body of email:

- *Would it be possible for you to complete a task for me before I leave for a meeting?*
- *Do you have time to run a quick errand?*
- *I need you to run a task at any store around you, I need some Apple Store gift cards to send out to a client today; how soon can you get them?*
- *Or find words like "KINDLY"*

Usually followed by a request to send money or purchase gift cards and that you will be reimbursed; ending with signature from the manager/supervisor. But could include also clicking on malicious links, etc.

FBI on Phishing, Etc.

- The FBI's Internet Crime Report for 2020 identifies by victim count, Phishing/Vishing/Smishing/Pharming as the top-ranked crime type with approximately 241,000 victims reported.
- Losses reported totaling approximately $54,241,000.
- Real estate industry and legal industry both a target.

BEC – What is it?

Business Email Compromise (BEC) is basically a type of phishing scam used by criminals to get a ***business email user*** to do something they should not, by, for example:

- Hacking into a business email account and impersonating the real owner or
- Using a spoofed domain to trick one into thinking he or she is communicating with the real owner.

BEC scams seemed to be more about interacting with victims (grooming them), rather than simply trying to dupe them in one attempt.

Key: It exploits trust.

BEC Attacks

Identify a Target

Usually using publicly available information

Step.1

Compromise Email Accounts/Domain Spoofing

.Attacking the email environment or sending an email using a modified domain

Step.2

Grooming

Targets the victim and gains trust

Step.3

Exchange of Information/Execute Scam

Finally perpetrating the scam to completion

Step.4

FBI on BEC Attacks

- In 2020, the IC3 received 19,369 BEC/EAC complaints with adjusted losses of over $1.8 billion
- Per the FBI – *They are sophisticated scams targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when the subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds…the scams evolved to include* ***spoofed lawyer email accounts*** *[and]* ***targeting the real estate sector****….*

SOME RED FLAGS MAY EXIST, FOR EXAMPLE:

- Who is it from – if supposed to be from CCapossela@CATIC.com yet shows as CCapossela@**abstractcompany.com** or as **CCapossela@CAT1C.com,** stop, ask why it shows a different domain name, verify and confirm!
- If says "Click Here" – hover over the URL. If it takes you to a random website that has nothing to do with the email, stop, ask why, verify and confirm!
- If have an attachment, hover over it. If it shows up as a URL, stop, ask why, verify and confirm!
- If the closing signature in the email is different than the actual sender email address, stop, ask why, verify and confirm!
- If there is a sense of urgency, stop, ask why, verify and confirm!
- Look for grammatical mistakes in email, and stop, ask why, verify and confirm!
- Look for certain words used like *Kindly*, and stop, ask why, verify and confirm!

BUT WHEN THE RED FLAGS DO NOT EXIST, STILL ALSO…

FOR EXAMPLE….

STOP AND YOU VERIFY AND CONFIRM USING A KNOWN INDEPENDENTLY VERIFIED PHONE NUMBER, SEPARATE FROM THE NUMBER IN THE EMAIL!

BUT ALSO….

AND SLOW DOWN AND ALWAYS THINK BEFORE ACTING…

Before clicking on a link

Before clicking on an attachment

Before providing credentials

Before providing confidential/ sensitive information

Before transferring funds

Ransomware Attacks

- Ransomware – basically malicious software, or malware, designed in part to deny access to a computer system or data until a ransom is paid. It also is a way for the criminals to steal data.

- Among other ways, ransomware typically spreads through phishing emails, software vulnerabilities or visits to an infected website.

- Recovery can be a difficult process, and there is no guarantee that you will recover files or data if you pay the ransom or what else the criminals may do with information they may obtain.

- FBI – does not encourage paying ransom, and regardless if you pay the ransom the FBI urges you to report an incident to the local FBI office. FBI's Internet Crime Report for 2020.

PLAN WITH YOUR EXPERTS

Some examples of things to consider for your review with your experts (not all-inclusive, needs vary):

- Proper preventative, detection, monitoring systems
- Proper firewalls
- Proper anti-virus/anti-malware/anti-pharming
- Proper backups and testing
- Multi-factor authentication
- Secure communication systems – for example, email; think multi-factor authentication and encryption
- Encryption (data in rest and in motion)
- Virtual Private Networks (VPN)
- Network Segmentation
- Requirements re: use of company's systems
- Limiting information you share online or on social media
- Email Plans
- Fund Transfer Plans
- Awareness Alerts/Acknowledgements/Training/Discipline
- Response Plans

What else?

- Monitor and Keep Up on Changes
- Modify When Necessary
- Obtain ***PROPER*** Cyber and Crime Coverages

Title Fraud (Deed Theft)

What is it?

Someone obtains title to your property – usually by stealing your identity.

How does it happen generally?

- Criminals select a house
- Gather information, for example, from internet ***or using social engineering techniques***
- Criminals take over your identity or claim to represent you
- Transfer ownership to themselves, using forged signatures and fraudulent identification
- Sell the home or borrow against the equity
- May pay the loan for some time so you are unaware

Title Fraud (Deed Theft)

Some Examples of Key Targets

- Unoccupied homes or rental properties
- Second homes, vacation homes
- Seniors
- Homeowners in crisis
- People who do not practice good cybersecurity measures

Title Fraud (Deed Theft)

How to Try to Mitigate the Risk, Some Examples (not all inclusive):

- Awareness
- Protect your personal information
- Follow proper cybersecurity measures
- Check property records
- Check credit reports
- Pay attention to incoming bills and your accounts
- Purchase proper insurance
- Think before you sign anything!
- Have a response plan

QUESTIONS


INSURANCE
BONDS
VOLUNTARY EMPLOYEE BENEFITS
SUCCESSION PLANNING

Thank You

101 Corporate Place, Rocky Hill, CT 06067
860-513-3131
email@CATICPro.com
www.CATICPro.com

CATIC
AGENT DRIVEN. INSURING RESULTS.

CATIC PRO INC.
PROFESSIONAL SOLUTIONS FOR YOUR BUSINESS