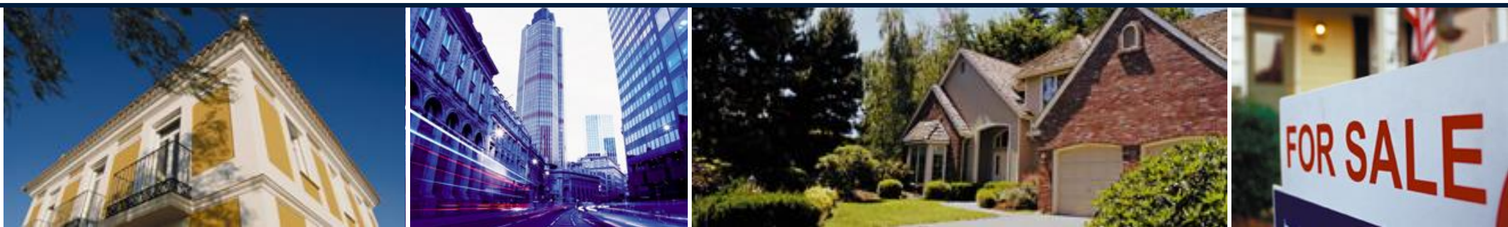
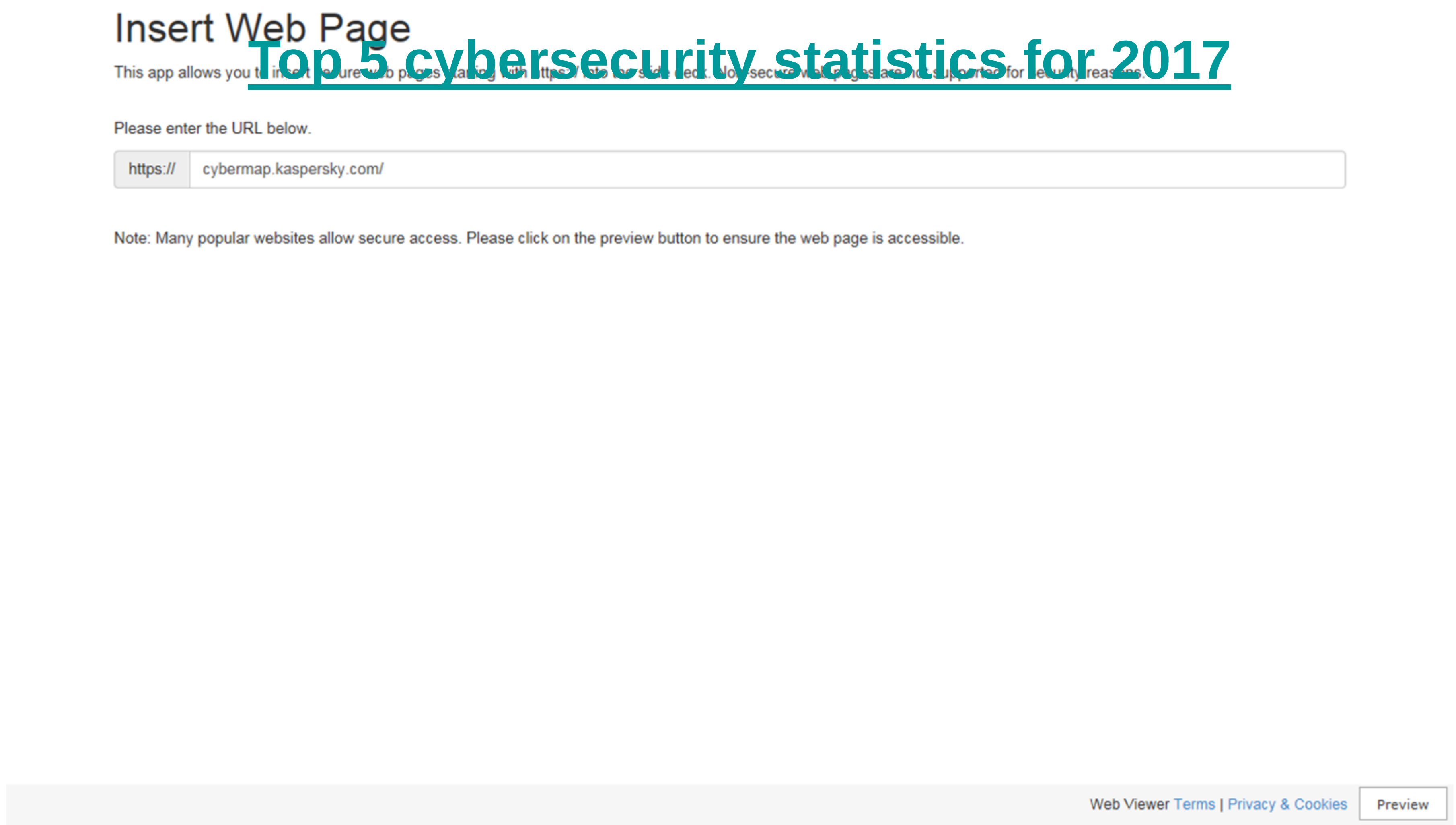
Data and Financial Transactions Security - What You Need to Know, Now!

Rick Diamond, VP, Agency I.T. Director, FNTG
rick.diamond@fnf.com
@rdiamondFNF

FIDELITY NATIONAL TITLE GROUP



Top 5 cybersecurity statistics for 2017



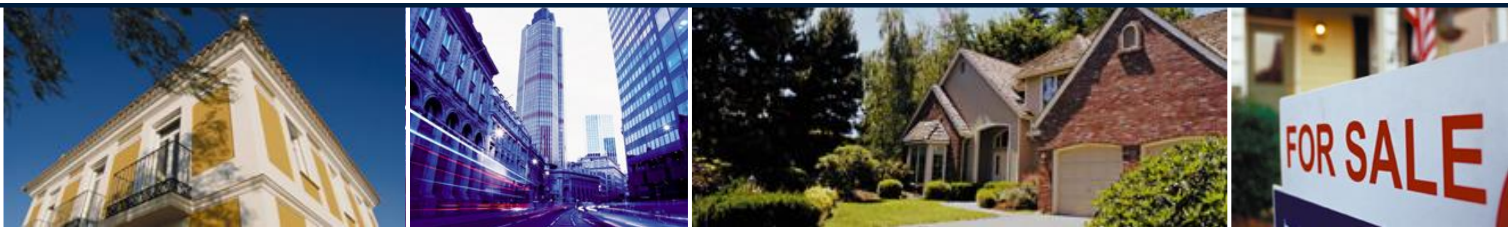
Insert Web Page

This app allows you to insert secure web pages starting with https:// into the slide deck. Non-secure web pages are not supported for security reasons.

Please enter the URL below.

https:// cybermap.kaspersky.com/

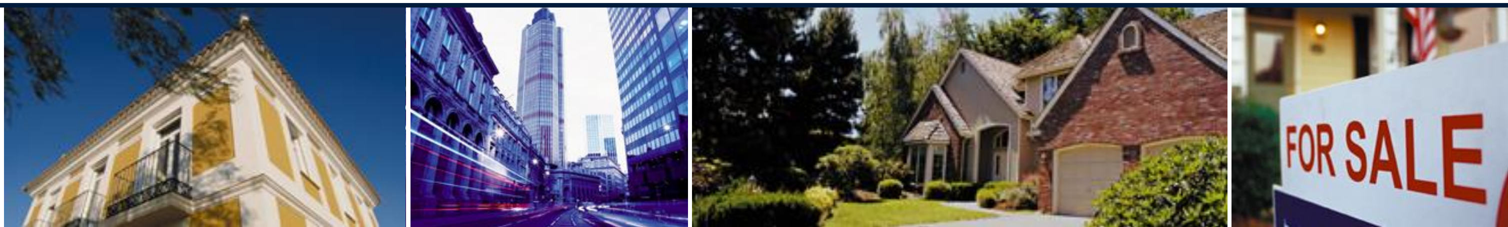
Note: Many popular websites allow secure access. Please click on the preview button to ensure the web page is accessible.



Why are you doing this and why should you care?

- Not because the cfpb wants you to…
- Not because your lenders want you to…
- Not because your underwriter wants you to…
- Not even because I want you to…

- You are doing this to protect yourself and your business!



Major Data Breaches

[redacted]

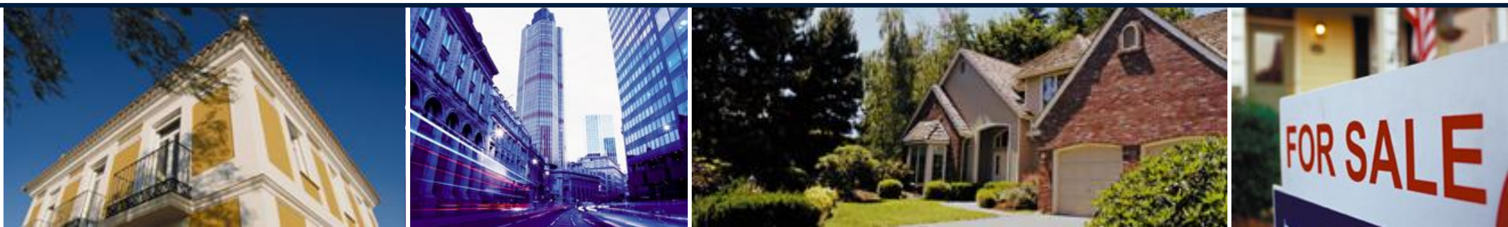
Are you Next?

[redacted]

Top 5 cybersecurity statistics for 2017

- Cybercrime damage costs to hit $6 trillion annually by 2021.
- Cybersecurity spending to exceed $1 trillion from 2017 to 2021.
- Unfilled cybersecurity jobs will reach 1.5 million by 2019.
- Human attack surface to reach 4 billion people by 2020…. *91%percent of attacks by cyber criminals start through email*
- Up to 200 billion IoT devices will need securing by 2020 *and there is some good news coming!*

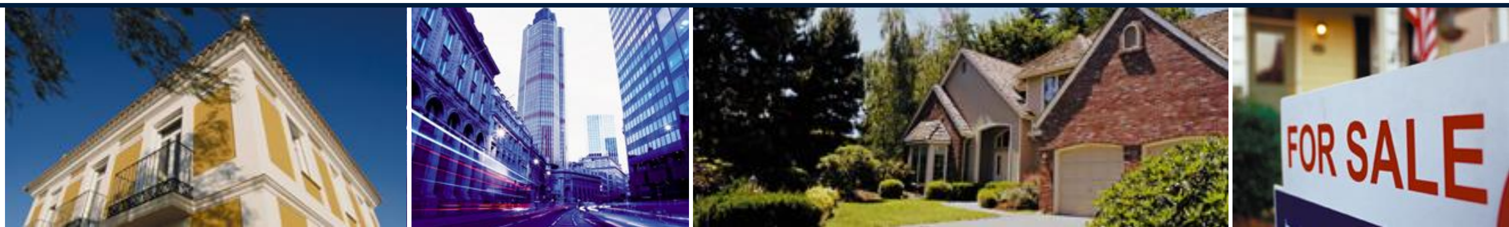
CSO
FROM IDG



Help is Coming in 2018 with Wi-Fi

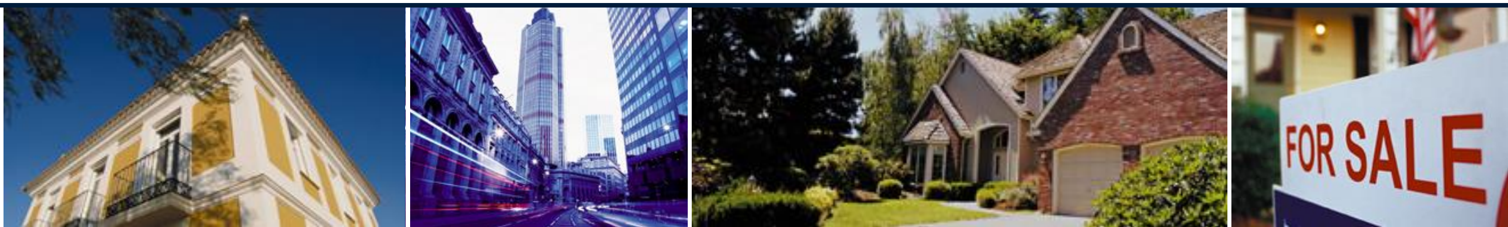
- WPA3 protocol strengthens user privacy in open networks through individualized data encryption.
- WPA3 protocol will also protect against brute-force dictionary attacks, preventing hackers from making multiple login attempts by using commonly used passwords.
- WPA3 protocol also offers simplified security for devices that often have no display for configuring security settings, i.e. IoT devices.
- Finally, there will be a 192-bit security suite for protecting Wi-Fi users' networks with higher security requirements such as government, defense and industrial organizatio

The Hacker News
Security in a serious way
www.thehackernews.com



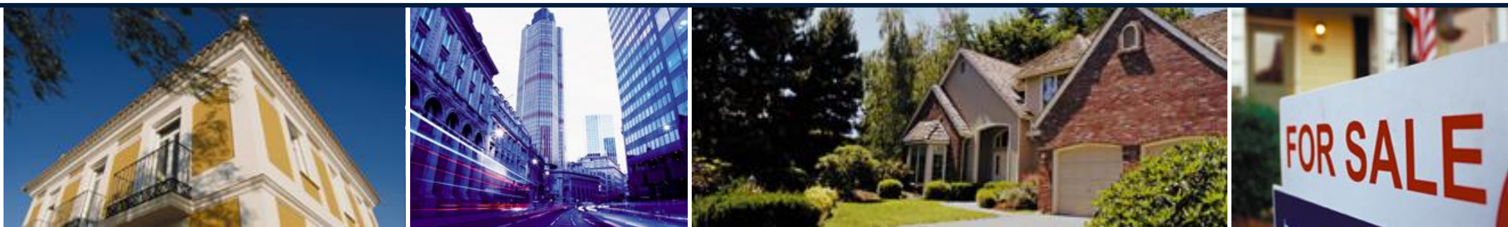
Think you’re Protecting your Data??

- Are e-mail and attachments encrypted? Is your data at rest encrypted?
- Are personal e-mail accounts restricted?
- Do you control the use of removable devices like flash drives?
- Do you destroy old hard drives of computers and copiers?
- Do you have audit and training procedures to insure that staff comply with security measures and procedures?
- Do you conduct background checks of employees?
- Do you have oversight of 4th party service providers to be sure they secure NPI?



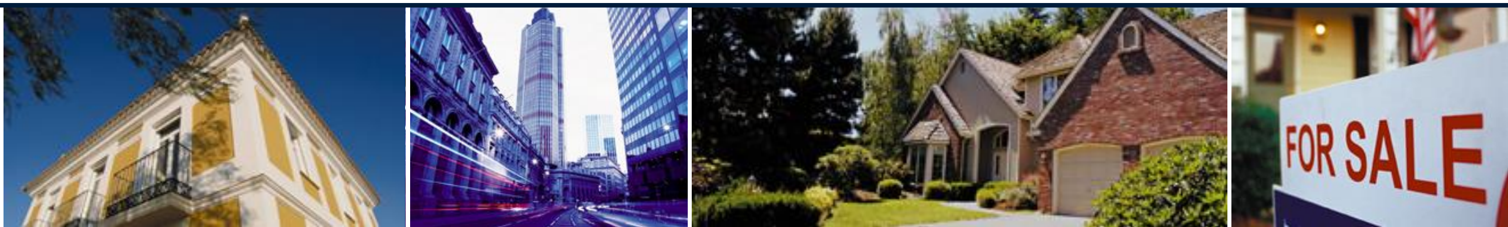
How important are background checks?

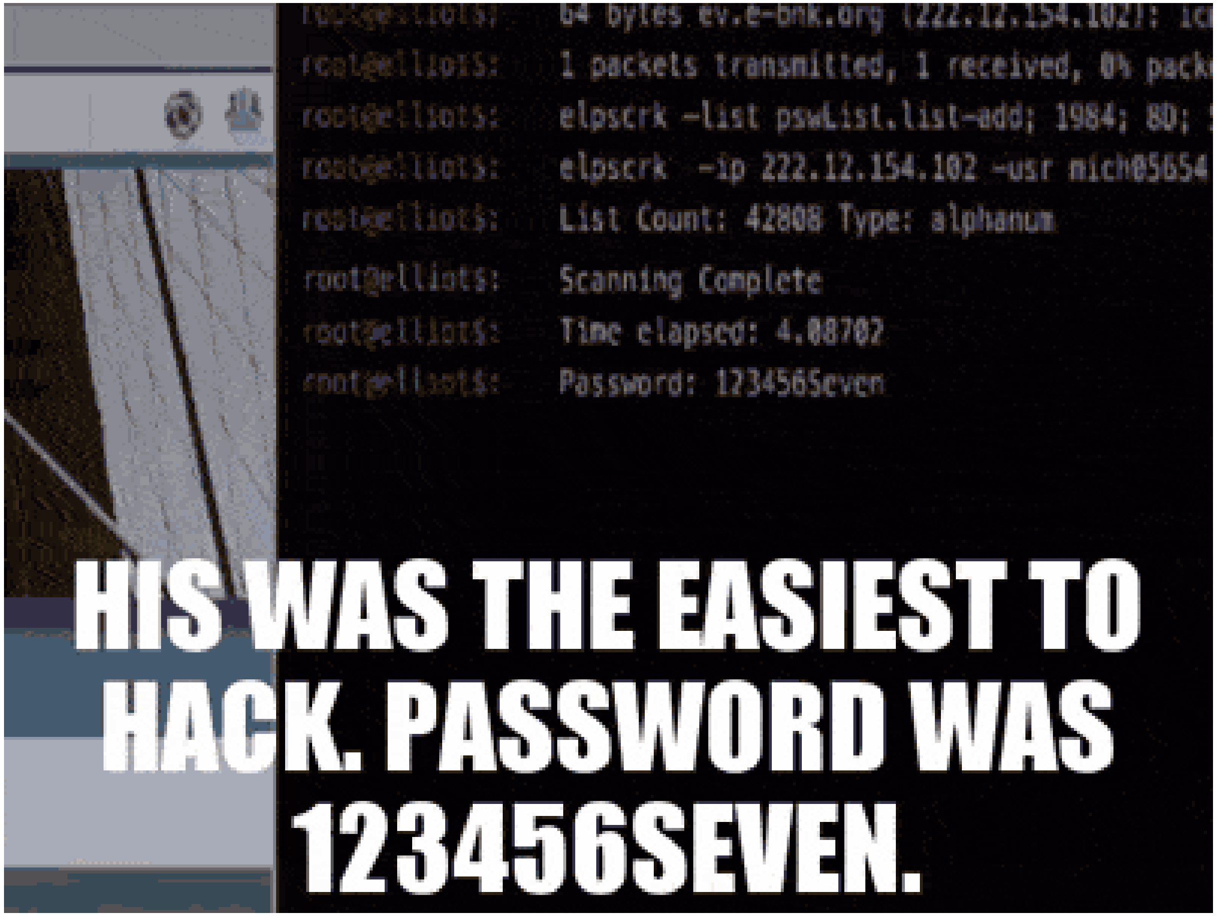
- Employees can access company's most sensitive data without having to circumvent security measures designed to keep out external threats.
- Besides selling their company's secret information, researchers also found evidence of rogue staff, in some cases, even working with hackers to infect their company networks with malware.



Those darn Passwords!

- Are you proactively managing your passwords?
  - Over 560 Million Passwords Discovered in Anonymous Online Database
  - In May 2016, LinkedIn had 164 million email addresses and passwords exposed
  - May 5th was World Password Day
  - Most stolen by Phishing attacks
  - *Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online*
  - Hackers know users cling to favorite passwords and weak passwords, resisting changing credentials regularly and make them stronger. It’s why attackers reuse old passwords found on one account to try to break into other accounts of the same user.

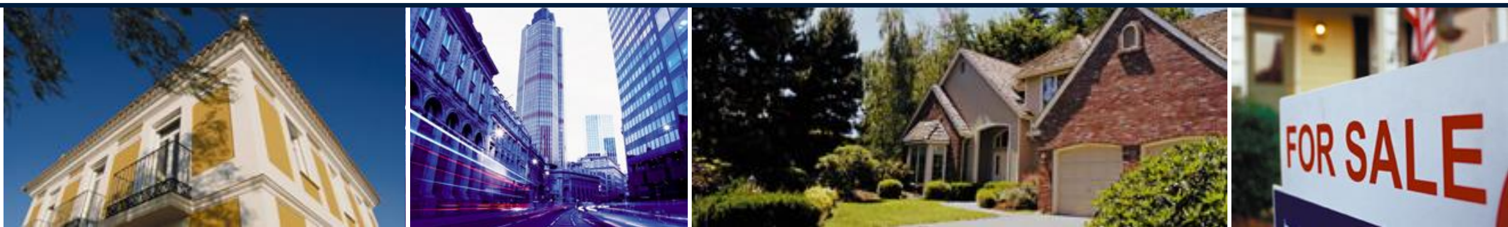




```
root@elliot$:   64 bytes ev.e-bnk.org (222.12.154.102): ic
root@elliot$:   1 packets transmitted, 1 received, 0% pack
root@elliot$:   elpscrk -list pswList.list-add; 1984; 80;
root@elliot$:   elpscrk  -ip 222.12.154.102 -usr mich05654
root@elliot$:   List Count: 42808 Type: alphanum
root@elliot$:   Scanning Complete
root@elliot$:   Time elapsed: 4.08702
root@elliot$:   Password: 123456Seven
```

HIS WAS THE EASIEST TO HACK. PASSWORD WAS 123456SEVEN.

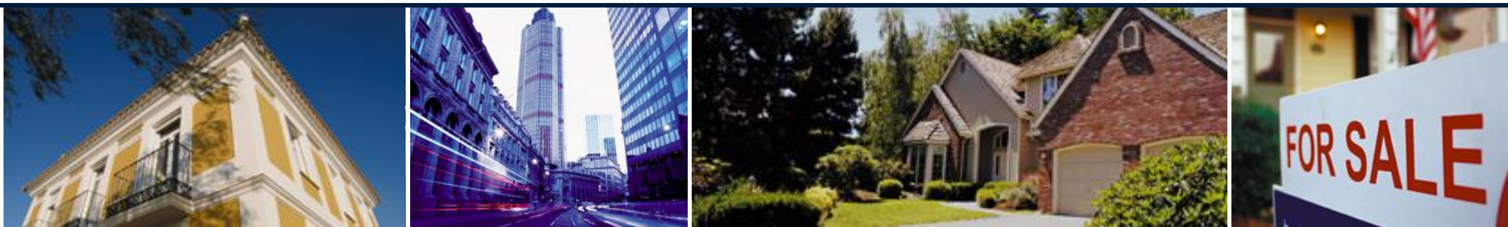
- What should you do to protect yourself and your company?

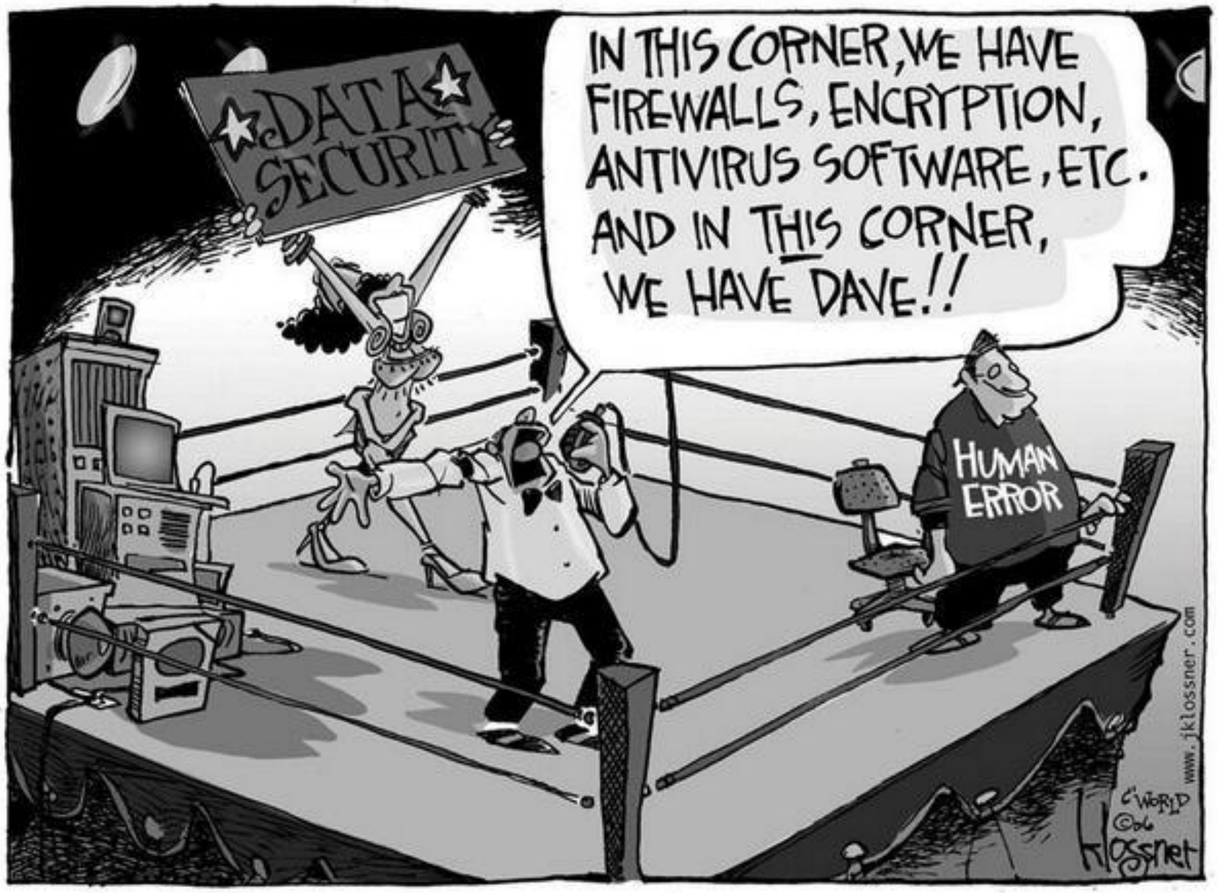


Those darn Passwords!

- Use strong and complicated *passphrases*
- Don't use the same passphrases for different accounts
- Change your passphrases frequently (60-90 days)
- Don’t share your password with anyone (especially family!)
- Use Multi Factor Authentication (MFA) to log in
- Microsoft will ban commonly used passwords from list of stolen ones
- A Password Manager can help
  - DashLane - https://www.dashlane.com/
  - LastPass - https://lastpass.com/
  - KeePass - http://keepass.info/

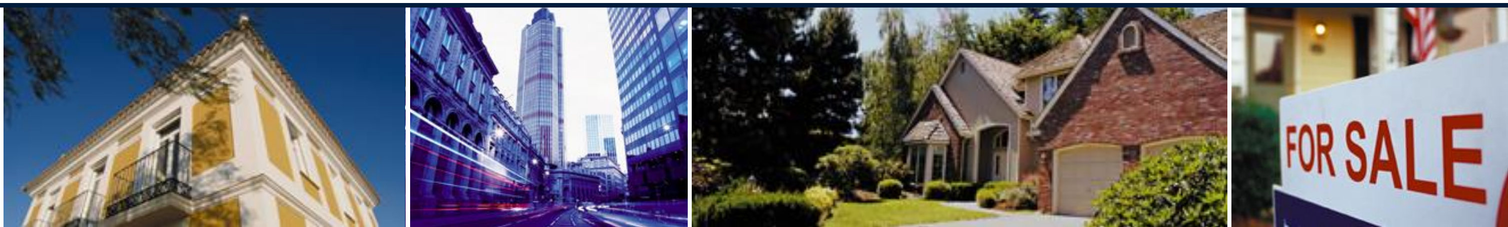
from c|net




IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
DATA SECURITY
HUMAN ERROR
www.jklossner.com
c'WORLD ©06
Klossner

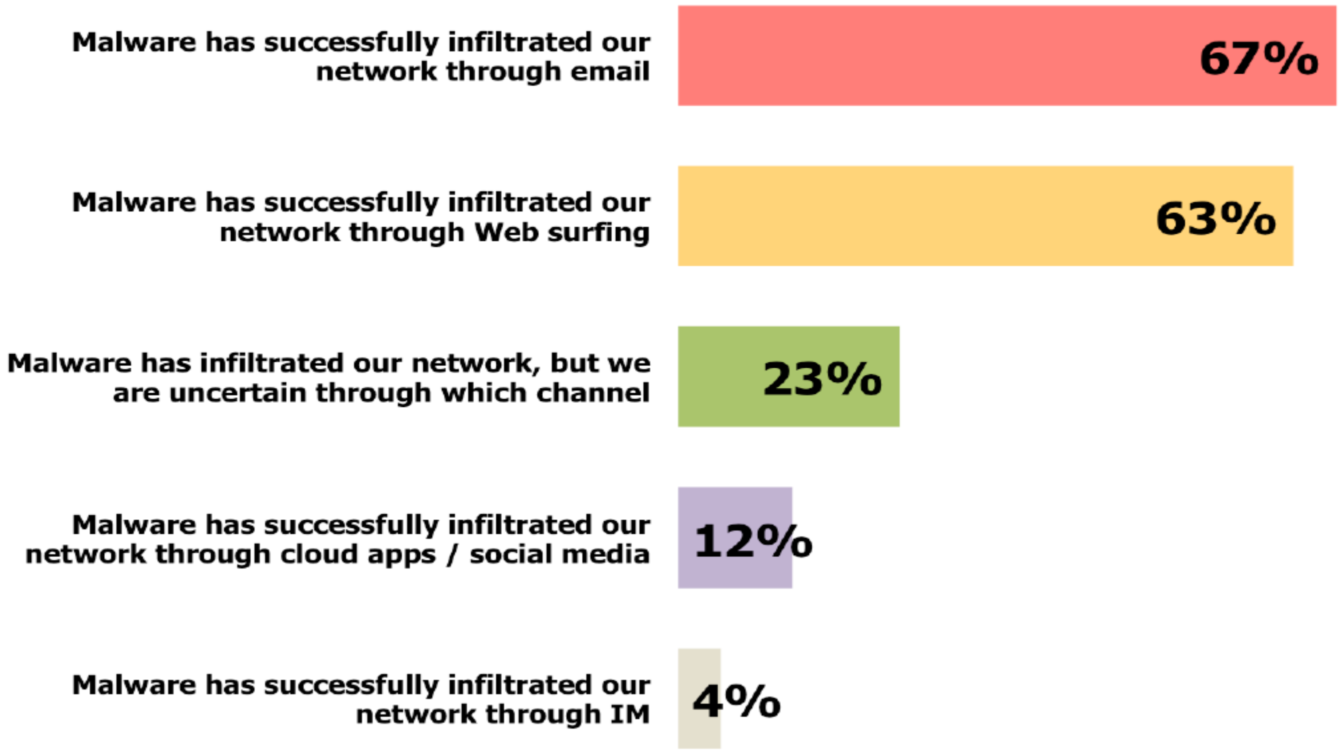
Hacking a human is by far the easiest way to get into a network!

Take this opportunity to educate your Realtors and clients!



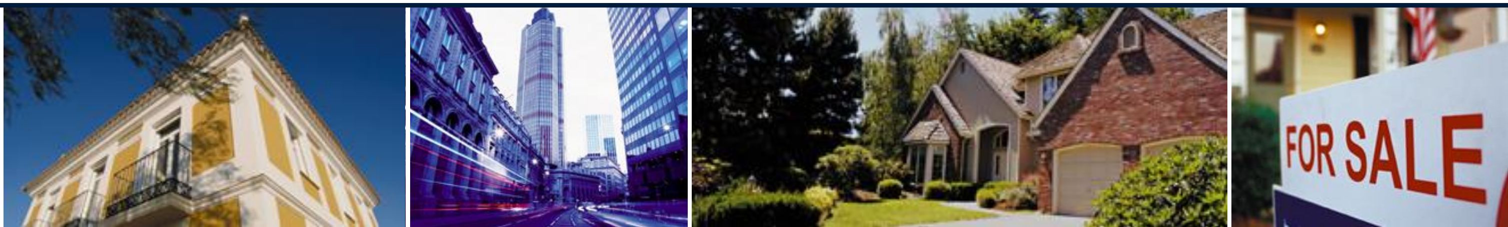
Is your Virus and Malware software up to date?

Malware Infiltrations That Have Occurred During the Past 12 Months



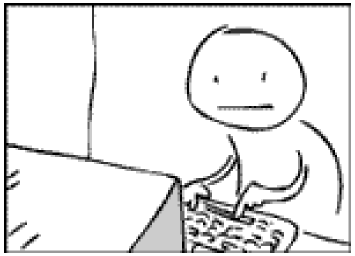
Source: Osterman Research, Inc.

- If it isn't…



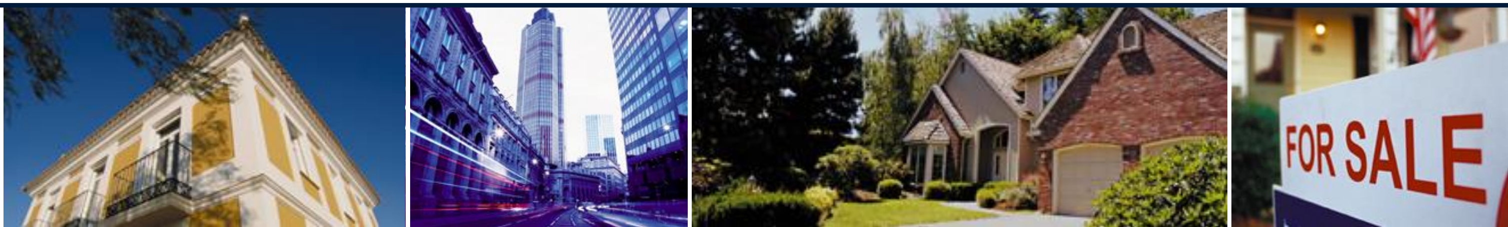
"*Dave*" strikes again!

- *Massachusetts* - Attorney was asked to stop ***payment*** on $635K in hacker scam using a fax *faxzero.com*
- *The scammer also called the paralegal yelling*
- Only a double checking phone call stopped this fraud!
- *Denver* – Buyer to Seller Wire gone! Buyer suing everyone!
- *Washington* - $1.6 Million gone! RICO claims and Treble damages!
- *California* – Chinese Nations impersonates a Chinese person $2.2 Million gone!
- 42% of Attorneys have experienced a virus or malware attack
- 60% of all Hacks are on small to mid-size businesses
- Remember, you are the low hanging fruit
- It only takes one breach to put an agent out of business



FBI - Internet Crime Complaint Center (IC3) https://www.ic3.gov

FIDELITY NATIONAL TITLE GROUP



FBI IC3: EAC Statistics

January 1,2016 to December 31, 2016

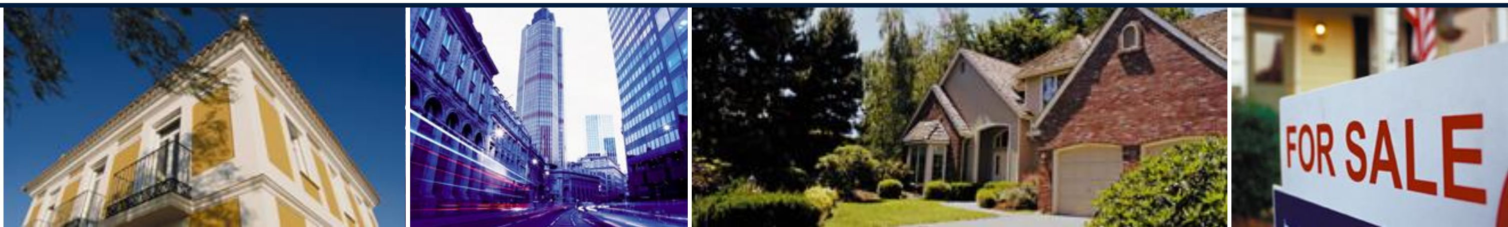
- Targeted Victims: Title Companies, Law Firms, Realtors, Sellers, Buyers

- 551 complaints filed by victims targeted during a real estate transaction

- 328 complaints were filed by **Title Companies**; 64% of all victims

- *https://www.fbi.gov/contact-us/field-offices/boston*

15 Constitution Dr,
Bedford, NH 03110
(603) 472-2224



Now you're a Target!

© Randy Glasbergen for Trend Micro

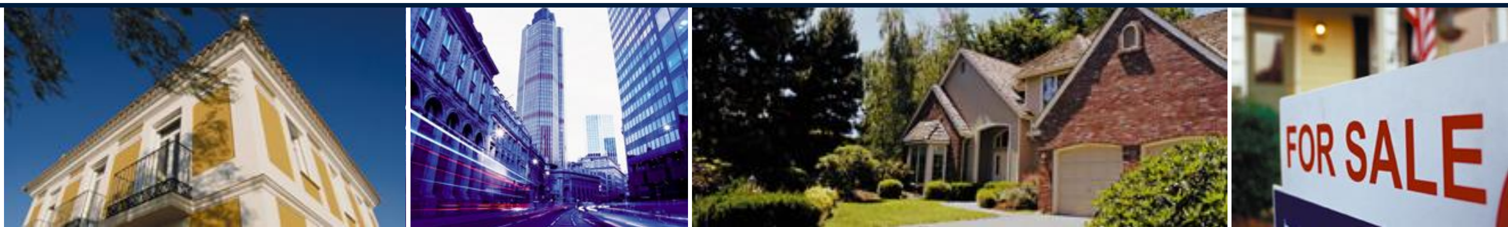
TREND MICRO

"On one hand, I'm grateful that we've never been targeted for a cyber-attack. On the other hand, I'm insulted that nobody thinks we're worth the effort!"

Where Cybercriminals will Attack Next

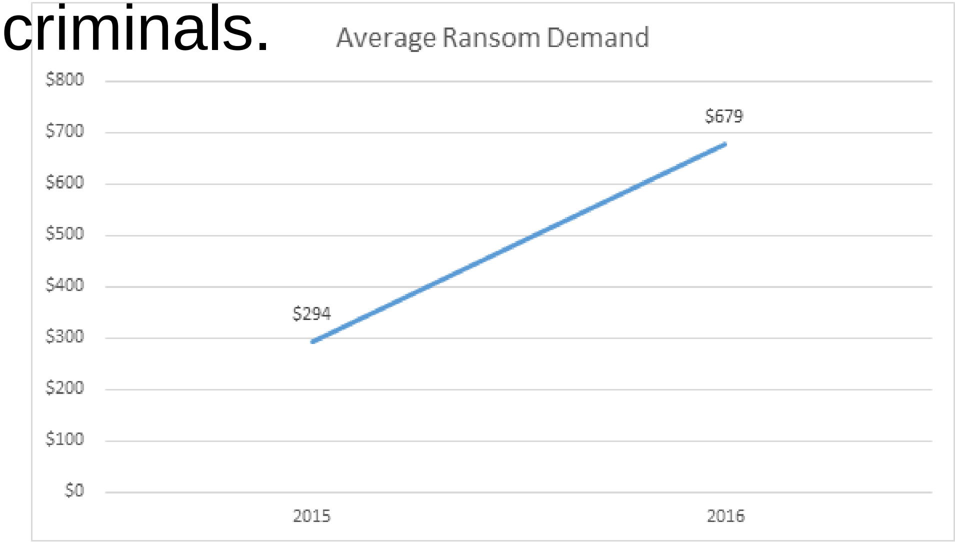
- Phishing – opening an attachment or clicking on a link
  - ➢93% of all Phishing is now Ransomware
- Spam – Corrupted Docs
- Compromised web site
- Malicious Downloads
- External Drives
- Future releases of Ransomware will need little or no user involvement
- Wire Fraud

CODE42

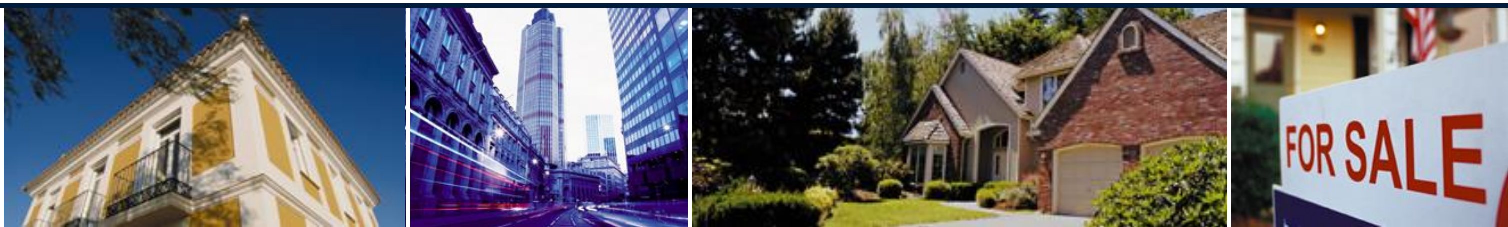


Growth of Ransomware into 2017

- Along with the growth of Ransomware distribution and infection, payments have also seen a growth. Approximately $209 million was paid to criminals in the first quarter of the year. FBI estimates are even higher. They expect $1 billion ransom to be paid out to cyber criminals.



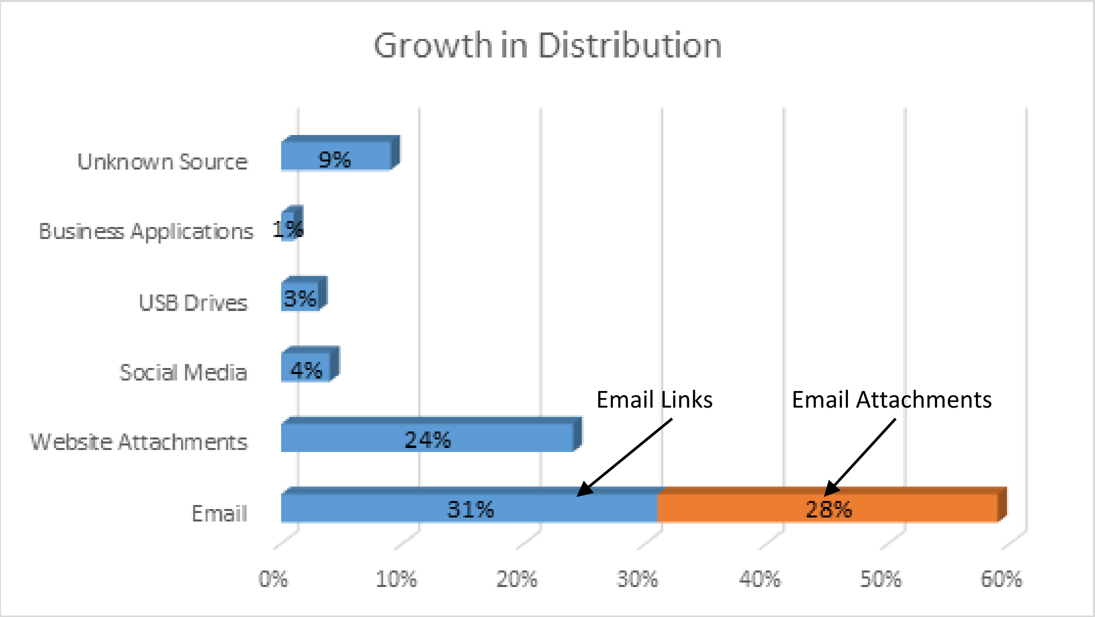
SYSTweak



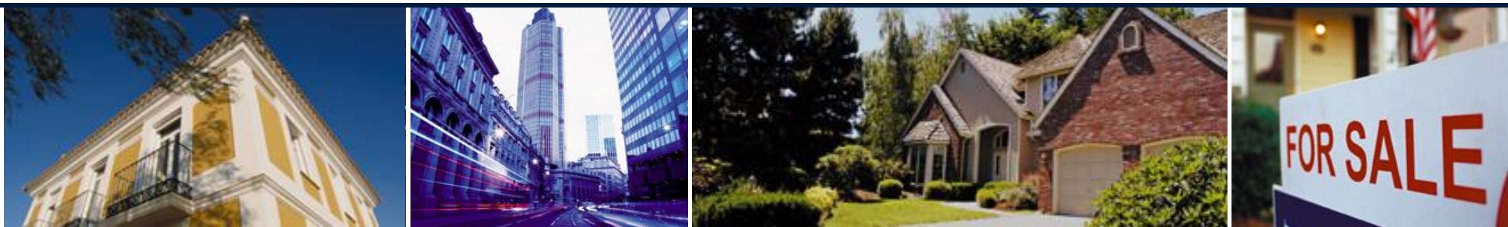
FIDELITY NATIONAL TITLE GROUP

Growth of Ransomware in 2017

- Criminals have taken up different mediums for distribution, including email, website attachments, social media, USB drives and business applications.
- Ransomware-infected emails expanded 6,000%

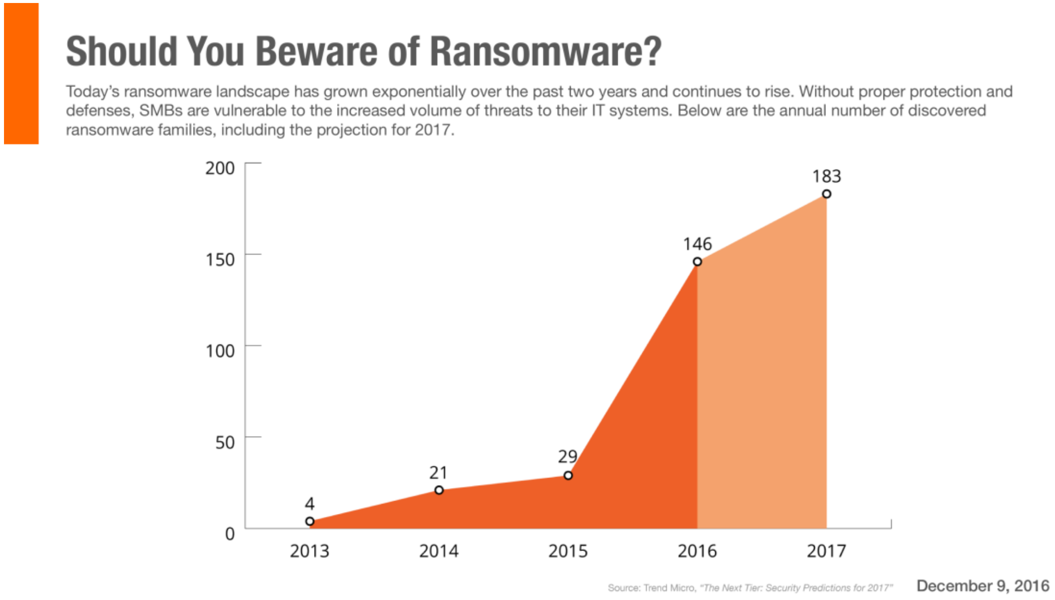


SYSTweak



Growth of Ransomware into 2017

- On an average, Ransomware infects 30,000 to 35,000 devices in a month. However, in March 2016 the Trojan variants managed to pollute 56,000 devices. *These devices also included Macs*

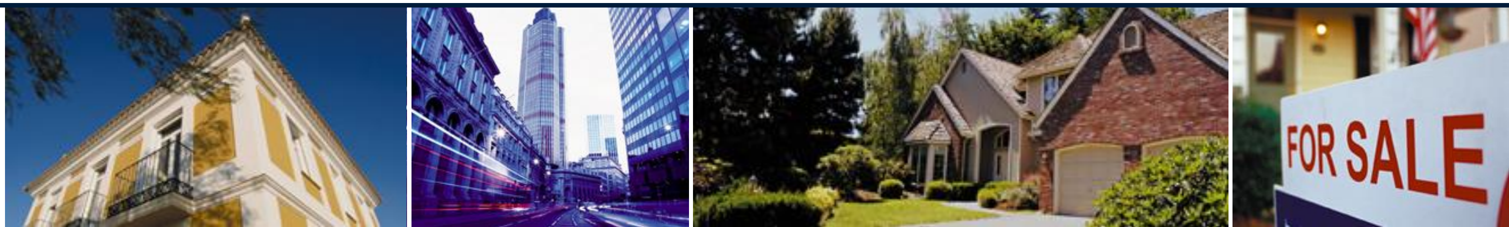


Should You Beware of Ransomware?

Today's ransomware landscape has grown exponentially over the past two years and continues to rise. Without proper protection and defenses, SMBs are vulnerable to the increased volume of threats to their IT systems. Below are the annual number of discovered ransomware families, including the projection for 2017.

Source: Trend Micro, *"The Next Tier: Security Predictions for 2017"*

December 9, 2016

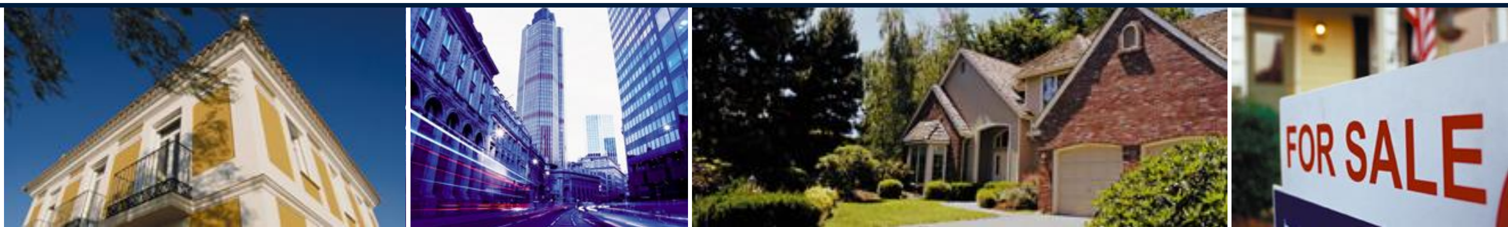


Ransomware - Don’t let this happen to you!

A Trifecta of mistakes!

- Mistake # 1 – Someone clicked on an infected link or attachment
- Mistake # 2 – Everyone was sharing and administrative login and password
- Mistake # 3 – Didn’t have proper backups

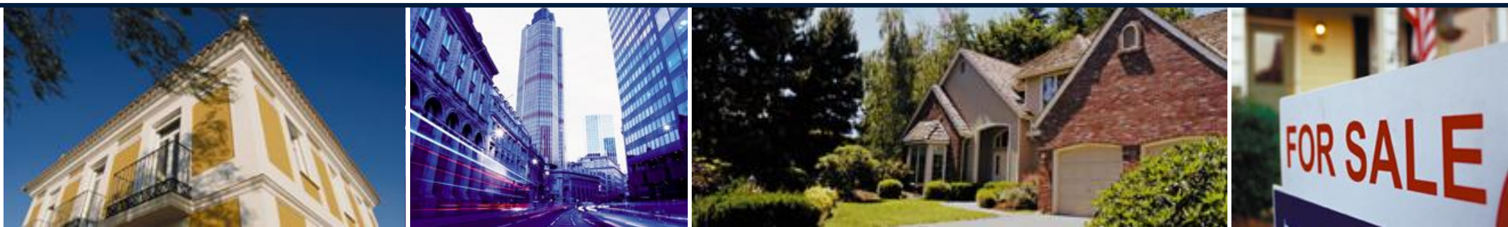
- Result? – They paid



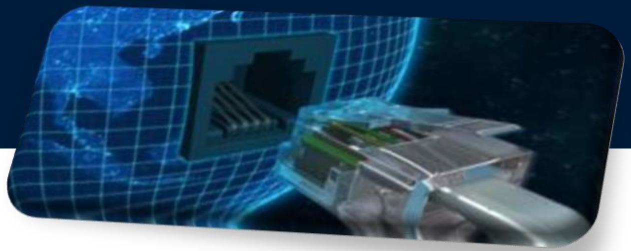
Ransomware is the New Normal

- **Global Ransomware Report 2018 found that ransomware is now something that more than half (56%) of companies have faced in the past two months.**
- **45% of US companies hit with a ransomware attack last year paid at least one ransom, but only 26% of these companies had their files unlocked. Companies paying the ransom were attacked again 73% of the time.**
- **(97%) said that they had backups for the files affected by the ransomware, and 51% said backups and the ability to self-recover were their reason for not paying the ransom.**
- **Backups!!!!**

Published by KnowBe4
CYBERHEISTNEWS
arming you with the facts



Cyber Liability



Cyber Liability provides coverage for the theft of your customers' non-public information
NOT the theft of your customers' escrow funds.

Cyber Liability provides coverage in the event you suffer a security breach, your customers' non-public information is compromised and they sue you for damages and expenses. These costs are covered under the following Cyber Liability policy insuring agreements:

- Security and Privacy Liability
- Privacy Regulatory Defense & Penalties
- Data Recovery - ***Ransomware***
- Customer Notification and Credit Monitoring Costs
- Data Extortion/Ransomware
- Multimedia Liability

RIEBLING
INSURANCE AGENCY, LLC

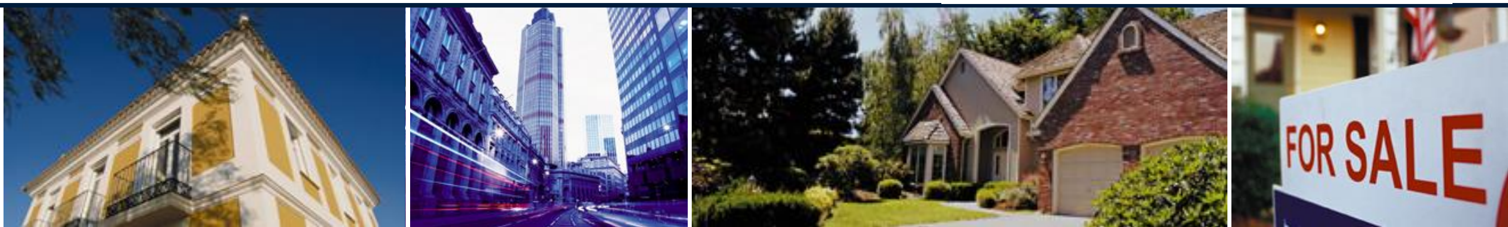
- Tier 1: $250K Limit = $328 Premium; $500K Limit = $472 Premium; $1M Limit = $652 Premium
- Tier 2: $250K Limit = $538 Premium; $500K Limit = $781 Premium; $1m Limit = $1,085 Premium
- Tier 3: $250K Limit = $712 Premium; $500K Limit = $1,038 Premium; $1M = $1,445 Premium
- Tier 4: $250K Limit = $888 Premium; $500K Limit = $1,296 Premium; $1Limit = $1,806 Premium

Patch! Patch! Patch!

EQUIFAX

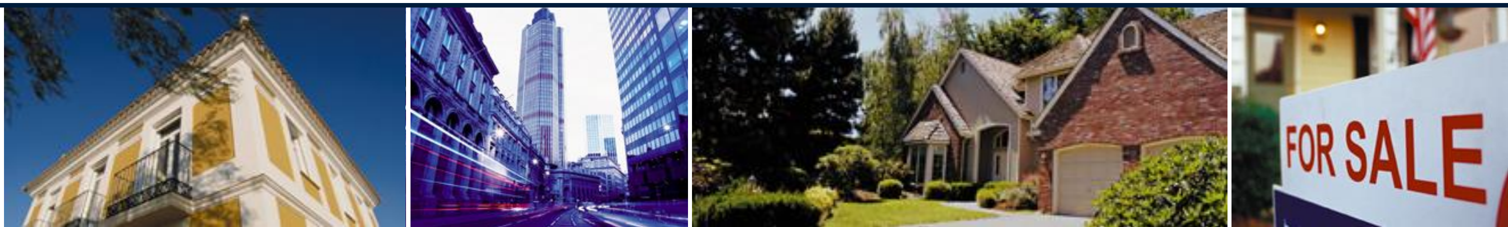
- Patching means applying available updates for operating systems and applications such as browsers, plugins, desktop apps, etc. They include both security and feature patches, and are meant to fix or improve the software you use.
- Software patching is one those proactive things we can do to enhance our security online.
- Patching software is like maintaining your car: It will still run without maintenance, but driving becomes more and more dangerous the longer you go on without a check-up.

HEIMDAL SECURITY



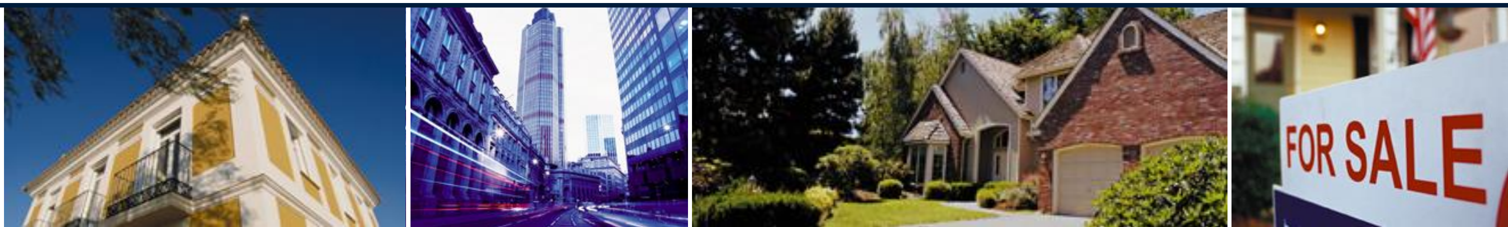
The 10 Most Dangerous Celebrities to Search in 2016

10. Ke$ha - 11.11%
9. Selena Gomez - 11.11%
8. Daniel Tosh - 11.56%
7. Chris Hardwick - 12.56%
6. Miley Cyrus - 12.67%
5. Rihanna - 13.33%
4. Will Smith - 13.44%
3. Carson Daly - 13.44%
2. Justin Bieber - 15.00%
1. Amy Schumer 16.11%



The 10 Most Dangerous Celebrities to Search in 2017

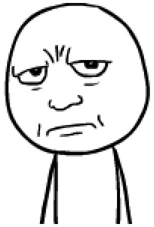
10. Beyoncé
9. Katy Perry
8. Diddy
7. Justin Bieber (only repeat celebrity)
6. Calvin Harris
5. Celine Dion
4. Zayn Malik
3. Carly Rae Jepsen
2. Bruno Mars
1. Avril Lavigne



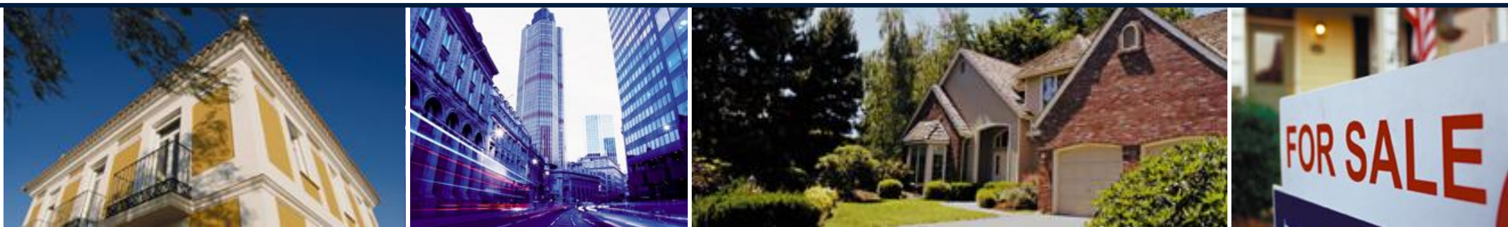
Lenders are Using this Opportunity to Ask

– Are you still using a “free” email service?

- ➢ Disproportionate amount of spam
- ➢ Your email may be viewed as spam
- ➢ Easier targets for Malware Attachments
- ➢ Yahoo hack – deleted and replaced wiring instructions!
  - ➢ Yahoo says at least 1 billion accounts were hacked in 2013 and 500 million in 2014. The stolen data includes users’ names, email addresses, telephone numbers, dates of birth, *hashed passwords*, and security questions for verifying an accountholder’s identity.
  - ➢ Hacked again – December 2016

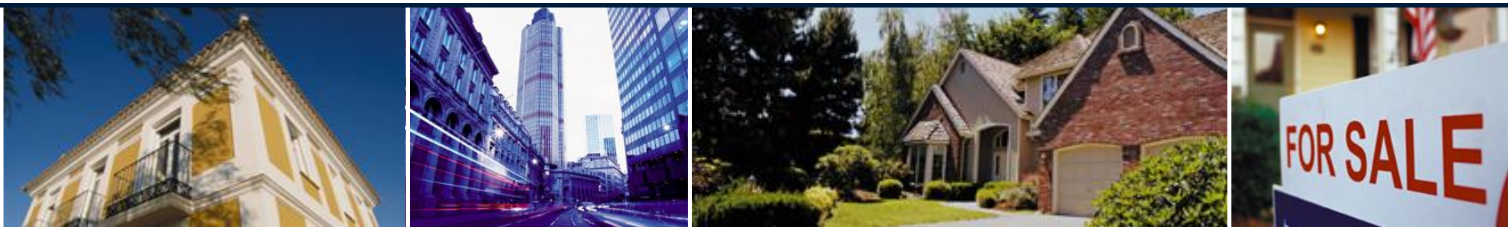


- ➢ AOL hack – agent not using added security feature
- ➢ email will remain the most important entry point for malware for the next several years
- ➢ Unprofessional



Phishing Advice

- Focus on detection and reporting of clicks, not just prevention
  - ➢Empower users to alert on “phishy” emails.
  - ➢Identify phishing recipients and recall/delete the email
  - ➢Identify phishing recipients who clicked the link or opened the attached file
  - ➢Expire credentials accessed from compromised host(s)
  - ➢Investigate post-click communications from any infected hosts
  - ➢Isolate the system so that malware cannot spread
  - ➢Identifies and removes the malware
  - ➢Prepend external emails with “Email from External Source”

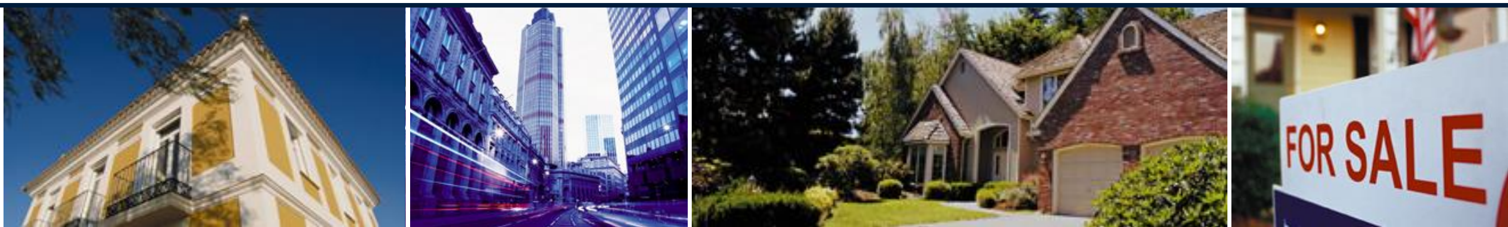


Professional Solutions

- GoDaddy Professional email - https://www.godaddy.com/email/professional-email

- Google email for your Business - https://www.google.com/work/apps/business/

- *This is also a good opportunity to review any E&O or professional liability insurance to confirm it covers cybercrime and data breach.*



Wire Fraud – Steps to Take

- There are three practices we would recommend all agents follow to protect against business email compromise:

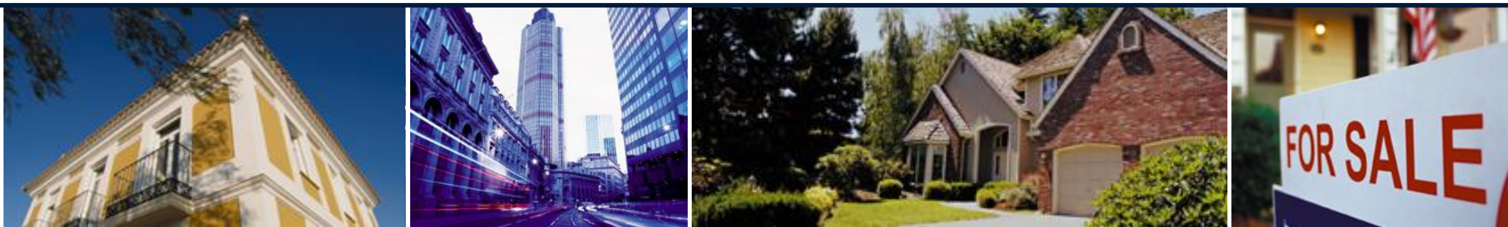
  1) only use email that provides two factor authentication and make sure it is enabled

  2) never wire funds based upon the content of an email. Always assume email has been hacked and validate all information over the phone

  3) if you suspect a wire or check was sent fraudulently, contact the bank immediately. Do not hesitate to respond

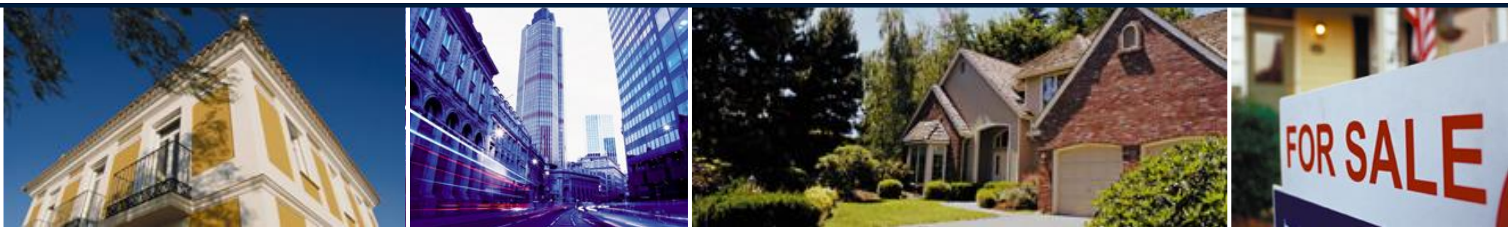
  4) I would recommend never allow wire instructions via email…phone or in person and CONFIRM even by phone!

Lender Routing # Verification ttps://routingnumber.aba.com



Hit by Wire Transfer Fraud? Use the Kill

- Criminals launder billions of dollars overseas through financial fraud schemes like wire transfer fraud, corporate account takeovers, business e-mail compromise scams and other financially motivated crimes.
- The FBI offers a Financial Fraud Kill Chain (FFKC) process to help recover large international wire transfers stolen from the United States.
- The FFKC is intended to be utilized as another potential avenue for U.S. financial institutions to get victim funds returned. Normal bank procedures to recover fraudulent funds should also be conducted.
  - ➢ The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:
  - ➢ the wire transfer is $50,000 or above
  - ➢ the wire transfer is international
  - ➢ a SWIFT recall notice has been initiated
  - ➢ the wire transfer has occurred within the last 72 hours.
- Any wire transfers that occur outside of these thresholds should still be reportec enforcement but the FFKC cannot be utilized to return the fraudulent funds.

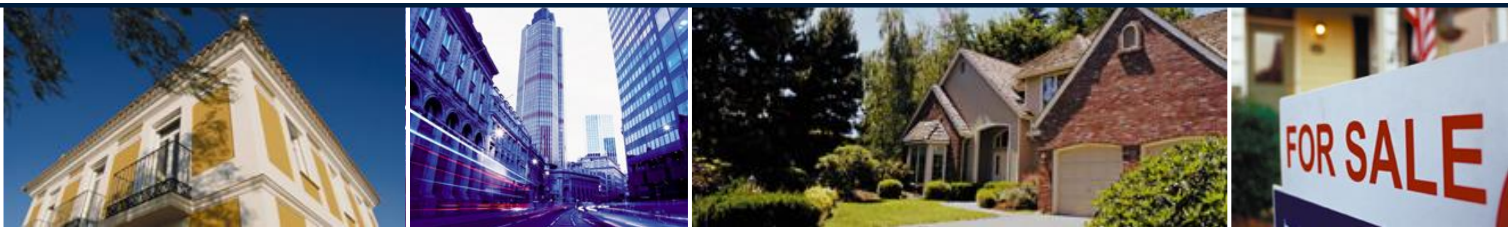


Backups, Business Continuity
Lenders are Using this Opportunity to Ask

- Are you thinking about Disaster Management and Business Continuity?

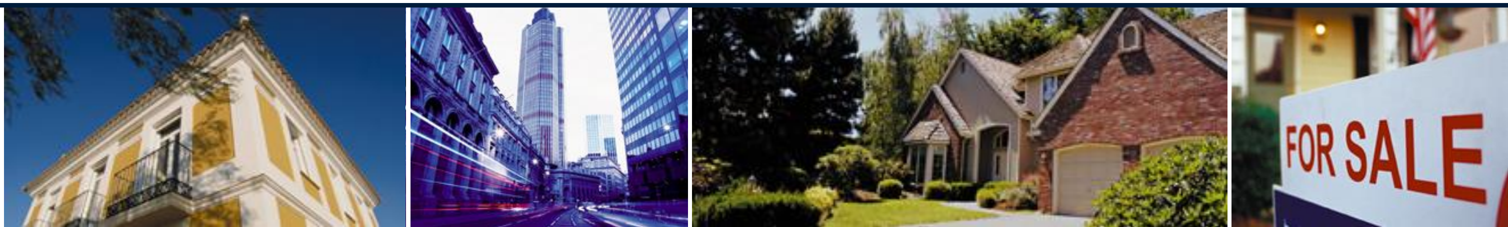
➢What are your backup procedures?
➢What is your Business Continuity plan?
➢Are they documented and tested?
➢Infrascale – https://www.infrascale.com
➢Carbonite – https://www.carbonite.com

Do you have a locally installed Production Software?



Third Party Hosting Companies

- Premier Data Services - www.PremierDataServices.com
- Google Cloud Platform - https://cloud.google.com/why-google/
- Amazon Web Services - https://aws.amazon.com/products/
- Premier One - http://www.premier-one.com/



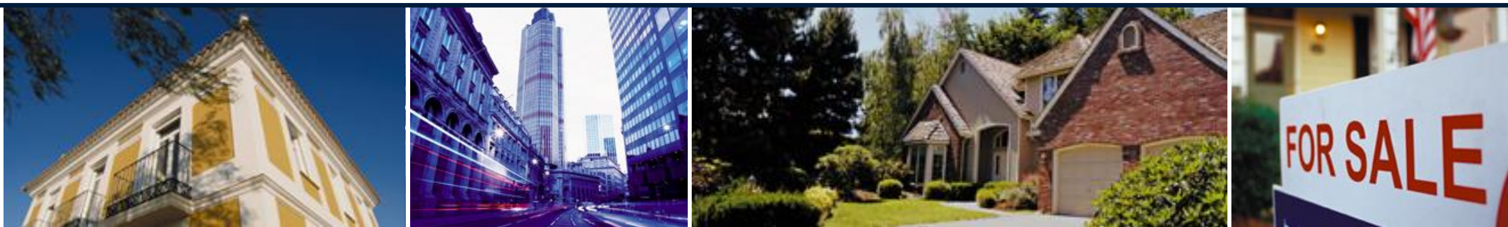
Realtor Resources

- Inman - http://www.inman.com/
  - ➢ Real Estate Technology News & Trends
  - ➢ Real Estate Marketing Ideas & Strategies
  - ➢ Real Estate Agent News
  - ➢ Coaching Corner

InmanNews
WHERE REAL ESTATE AND TECHNOLOGY CONNECT

- Breakthrough Broker - http://www.breakthroughbroker.com/
  - ➢ Marketing - Easily create marketing material in minutes (Free)
  - ➢ Planning - Business and marketing plans for agents
  - ➢ Lead Generation - Strategies to help you grow your business
  - ➢ Social - Everything agents need to market their business using social media.
  - ➢ $395 per month

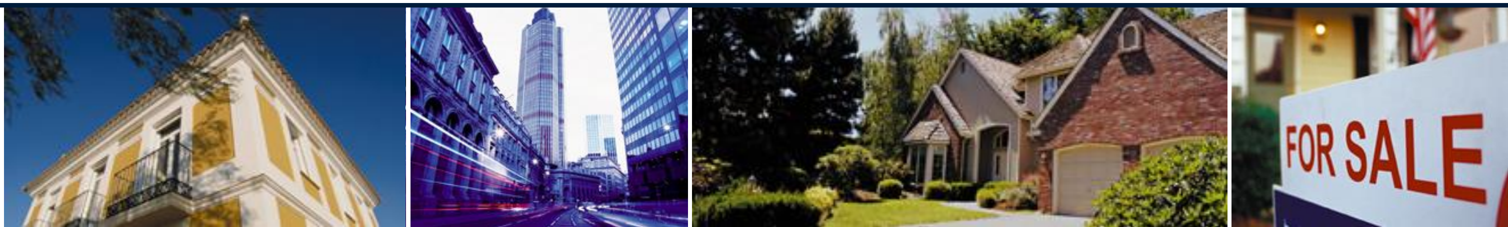
Breakthrough™
BROKER.com



Useful APPS

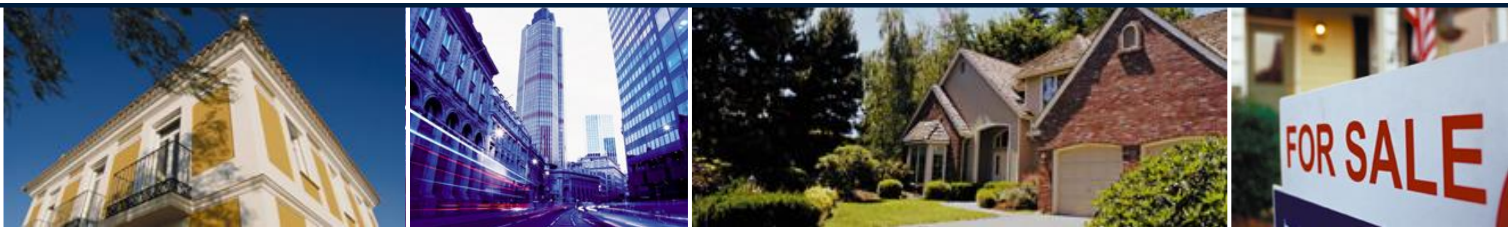
- The Hacker News - http://thehackernews.com/
- Any.do - To-Do List, Daily Task Manager & Checklist Organizer
- LastPass - remembers all your passwords, so you don't have to
- Firefox Focus - automatically blocks a wide range of online trackers
- Flipboard - gathers together news, popular stories and conversations
- Sideline – Free second telephone number on your phone
- SlyDial – Go directly to someone’s voicemail
- Fraud Fighter - https://www.fraudfighter.com/

- @rdiamondFNF



This Doesn’t Have to be Overwhelming

- Most of these things are easily accomplished and not overly expensive
- Remember Backups and Business Continuity
- This is a Journey not a Destination
- Remember all this PROTECTS YOU TOO!
- Start thinking about the next big thing…
  - *Bitcoin, Blockchain, eClosings*



Bitcoin

QUESTIONS?