How Technology Can Ruin Your Real Estate Business

Data Security, Tech Risk Management & Safety

Intro to Data Security & Tech Risk Management

Note: See glossary in back of note packet for definitions of different kinds of viruses & malware

How to Get & Avoid Viruses/Malware

1. **Non-Comprehensive Anti-Virus Protection** (Avast.com, MalwareBytes.com or AVG.com)

2. **Weak/Outdated (non-patched) programs**

On Windows - Windows 10 Updates Automatically, but if you have an older OS (Windows 8 or 7) you need to set up **Automatic Updates**:

1. **Control Panel > System & Security > Windows Update**
2. Click on **Change Settings** to set up **Automatic Updates**

On a Mac

Go to **Apple menu > System Preferences > App Store > select Automatic Updates** checkboxes

Software - make sure your Anti-Virus suite monitors software updates

Mobile Apps - make sure your App Store settings are to automatic updates

3. **Weak or Repeated Passwords**(Password Manager like LastPass.com or Base Psychology Method)

Base Psychology Password

Base Same on Every Site (but needs to be weird and random)	**+ Psychology** 1 Word that makes You Think of Each Site	**+ Quarter/Year** (allows you to easily update throughout the year)
2Sr1pMx	zuck = facebook gmail = gmail aol = aol mls = mls	Q2 Q3 Q418
for example facebook would be 2Sr1pMxzuckQ418, mls would be 2Sr1pMxmlsQ418 ...then in January they would be 2Sr1pMxzuckQ119, mls would be 2Sr1pMxmlsQ119		

4. **Phishing Techniques** (broad & spear including wire transfer fraud)

Slow Down & Pay Attention and Look for Anything Out of the Ordinary such as:

- Mismatching Header Info *(ex. from: mike@microsoft.com but not really from microsoft)*
- Poor spelling or grammar
- Odd urls/links (ex. banko.famerica.com)
- Being greedy and wanting unexpected information

4 Steps to Defend Yourself & Your Clients from Wire Transfer Fraud

1. Educate your client about phishing techniques & what to look for

2. CYA:
    - Educate your client about wire transfer fraud
    - Get them to sign a disclosure form
    - Consider adding a wire transfer dislosure statement to your email signature
3. Pick the best vendors
    - Make sure they involve phone calls
    - Create a contact on your clients phone with their contact info
    - Instruct them to only accept calls and/or hang up and initiate the call with the contact you had them create
    - Make sure they have Cyber Insurance
4. Make sure you/your company has Cyber Insurance

5. Encryption - Process of encoding data in such a way that only authorized parties can read it)
Files & Folders on Your Computer

On Windows	**On a MAC**
1. Right click your mouse over a folder & click on **Properties** 2. From the **General Tab** click **Advanced** 3. Click **Encrypt Contents to Secure Data**	1.Open **Disk Utility** 2.Click on **File** > **New Image** > **Image From Folder** 3.Select the folder you want to encrypt, and click **Image** 4.Choose **'read/write'** & choose '**128-bit AES encryption**' if you want the contents of the folder to be editable
Other Options include: VeraCrypt, BitLocker, GNU Privacy Guard, 7-Zip	

Encryption in the Cloud - BoxCryptor.com (free for 1 account, $48/yr for unlimited accounts)

Encryption on Mobile (lock screen, bio-metrics, find your device @ icloud.com or google.com/android/find)

Encrypt Emails (Mailvelope browser extension)

---

6. Social Engineering

Remove info from Your Google Search Results https://goo.gl/o9MUBK

alerts.google.com, socialmetion.com or talkwalker.com

Periodic Cleansing of Your Social Media Life (review prior content, settings and assess friends/connections)

How Technology Can Ruin Your Real Estate Business

Data Security, Tech Risk Management & Safety

7. General Tech Safety Tips

E-Mail Security Tips

- Realize Your online activity creates SPAM
- Have 3 Different email accounts (business, personal, online usage) and let the 3rd one get all the spam
- Don't Click on Anything Anymore unless you know its legit/safe, especially financial emails
- Be careful of Unsubscribe links unless you were the reason the email started in the first place
- Be careful providing Private or Trusted info via email (and if you have to encrypt it)

Internet Security Tips

- Make sure your Anti-Virus is installed in Your Web Browsers
- Be careful of any site your Anti-Virus flags as a concern
- Be careful of any site that asks you to install something or download a folder of files if you don't know the source is safe
- If concerned, make sure the page has SSL: https: and icon of a closed lock

---

Computer Security Tips

- Use some common sense, if something seems to be good to be true (free), it usually isn't
- Make sure you are backed up at all times to the cloud (Carbonite.com or Google Drive Sync)

Personal Security Tips (BSafe app)

- Back up text messages (Export Messages for iOS or SMS Backup & Restore for Android)
- Solve Batter Issues with Battery Doctor app
- Always have a strong password on your home/office wi-fi
- Be careful using wi-fi at high traffic, public locations (airports, coffee shops, hotels, etc.)
- How to be safe using the Internet in public
    - Personal Hotspot
    - Virtual Private Network (VPN)
    - Air Card or Shared Hotspot
- Be careful of tech distractions and use the BSafe for You app to protect yourself in the field

---

---

8. Legal Risk Management

State Laws Online Display & Disclosure Laws & the NAR Short Messaging Exception Rule

Federal Laws

Can-spam Act of 2003 & the Junk Fax Prevention Act

Electronic Signatures - Uniform Electronic Transaction Act

Copyright Infringement (search.creativecommons.org, pixabay.com or fotolia.com)

9. NAR Policies

Local MLS & IDX Rules

Code of Ethics & Fair Housing

a. Article 1-9

b. Article 9-1

c. Article 12

e. Article 15

f. Fair Housing

10. Online Reputation Management & Etiquette

Anything you do digitally is:

1. Open to Each Person's Interpretation & Tone
2. Permanent Record
3. Easy to Distribute

Additional Notes:

How Technology Can Ruin Your Real Estate Business

Data Security, Tech Risk Management & Safety

Glossary

Virus - A type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected"

Kinds of Viruses

Resident vs. non-resident viruses - A *memory-resident virus* (or simply "resident virus") installs itself as part of the operating system when executed, after which it remains in RAM from the time the computer is booted up to when it is shut down. Resident viruses overwrite interrupt handling code or other functions, and when the operating system attempts to access the target file or disk sector, the virus code intercepts the request and redirects the control flow to the replication module, infecting the target. In contrast, a *non-memory-resident virus* (or "non-resident virus"), when executed, scans the disk for targets, infects them, and then exits (i.e. it does not remain in memory after it is done executing).

Macro viruses- Many common applications, such as Microsoft Outlook and Microsoft Word, allow macro programs to be embedded in documents or emails, so that the programs may be run automatically when the document is opened. A *macro virus* (or "document virus") is a virus that is written in a macro language, and embedded into these documents so that when users open the file, the virus code is executed, and can infect the user's computer. This is one of the reasons that it is dangerous to open unexpected attachments in e-mails.

Boot sector viruses - *Boot sector viruses* specifically target the boot sector/Master Boot Record (MBR) of the host's hard drive or removable storage media (flash drives, floppy disks, etc.)

Stealth Strategies - In order to avoid detection by users, some viruses employ different kinds of deception. Some old viruses, especially on the MS-DOS platform, make sure that the "last modified" date of a host file stays the same when the file is infected by the virus. This approach does not fool antivirus software, however, especially those which maintain and date cyclic redundancy checks on file changes

Read Request Intercepts - Some viruses trick antivirus software by intercepting its requests to the OS. A virus can hide itself by intercepting the request to read the infected file, handling the request itself, and return an uninfected version of the file to the antivirus software. The interception can occur by code injection of the actual operating system files that would handle the read request. Thus, an antivirus software attempting to detect the virus will either not be given permission to read the infected file, or, the read request will be served with the uninfected version of the same file

Self-Modification - Most modern antivirus programs try to find virus-patterns inside ordinary programs by scanning them for so-called *virus signatures*. Some viruses employ techniques that make detection by means of signatures difficult but probably not impossible. These viruses modify their code on each infection. That is, each infected file contains a different variant of the virus.

Encrypted Viruses - One method of evading signature detection is to use simple encryption to encipher the body of the virus, leaving only the encryption module and a cryptographic key in cleartext

Polymorphic code - was the first technique that posed a serious threat to virus scanners. Just like regular encrypted viruses, a polymorphic virus infects files with an encrypted copy of itself, which is decoded by a decryption module. In the case of polymorphic viruses, however, this decryption module is also modified on each infection. A well-written polymorphic virus therefore has no parts which remain identical between infections, making it very difficult to detect directly using signatures.

Metamorphic Code - To avoid being detected by emulation, metamorphic viruses (often large, complex and are triggered by a metamorphic engine) rewrite themselves completely each time they are to infect new executables.

How Technology Can Ruin Your Real Estate Business

Data Security, Tech Risk Management & Safety

Malware

Trojan horses - is any program that invites the user to run it, concealing harmful or malicious code. It is one of the most common ways that spyware is distributed, by bundling the undesirable piece of code along with a more desirable software you download &/or install (or by tricking the user with confusing end-user license agreements). The code may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or installing additional harmful software

Rootkits – allows a malicious program to remain concealed or avoid detection (or routines to defend against their removal) once it is installed on a system by modifying the host's operating system, file structure, list of processes, etc. so that the malware is hidden from the user &/or anti-virus program.

Backdoors - a method of bypassing normal authentication procedures. Once a system has been compromised, one or more backdoors may be installed in order to allow easier access in the future. Backdoors may also be installed prior to malicious software, to allow attackers entry. Backdoors secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors crackers may use Trojan horses, worms, Implants or other methods.

Computer Worm - is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Ransomware - restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed.

Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system (i.e. exploiting a known vulnerability, password (either by cracking, privilege escalation, or social engineering)). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root/Administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Keylogging - is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored

Dialers - are designed to connect to premium-rate numbers by leveraging security holes in the operating system installed on the user's computer and use them to set the computer up to dial up through their number, so as to make money from the calls.

Spyware - software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

Adware/**Advertising-Supported Software** - is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process. The functions may be designed to analyze which Internet sites the user visits and to present advertising pertinent to the types of goods or services featured there.

How Technology Can Ruin Your Real Estate Business

Data Security, Tech Risk Management & Safety

Rogue-AV or **Rogue security software** - is a form of Internet fraud using computer malware that deceives or misleads users into paying money for fake or simulated removal of malware (so is a form of ransomware)—or it claims to get rid of, but instead introduces malware to the computer.

GovWare - computer software or hardware created by a State or private companies working for the State to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Govware may take the form of malware,spyware, covert sensors, implants, or other invasive technologies.