Cyber Security for Real Estate Professionals Outline

Who am I ?

- Tim Crandall, IT Professional with 10 years plus of experience.
  - Degree in Broadcast Engineering (the science of radio waves) hence why I am called “the WiFi Guy”
  - Currently working on ISC Cyber Security Certification
  - 6 years as Crestron Programmer
- Why listen to my advice?
  - Because I am in it every day, I spend several hours a week just reading up on the new vulnerabilities/threats discovered- then try to figure out if any action is necessary for clients on retainer.
  - I don’t don’t do audio/video, cameras, access control, website design, etc- I focus my attention on one area alone- Networking/Security.
  - I am not alone, I have colleagues in the business I talk to and bounce ideas off of- and, because not one of us knows everything.

What part do I play in protecting ROGMC?

- Hardware / Networking
  - Hardware Firewall has been installed that uses the US Government List of threats/ malicious traffic and compares it to traffic going over the network- when it finds a match, it instantly blocks it.
- Consultation
  - Available resource when the need arises. 2 business day turnaround or less on questions in regards to network/security issues. Immediate (usually within 2-4 hours or less) for clients on retainer
- Education
  - This class, for instance!

Why do cyber criminals target real estate professionals?

- Outright theft
  - Criminals are looking for a quick payday- large financial transactions are a natural target (i.e. Debit/Credit card numbers, Checking account numbers, bank transfer information, etc)
- Identity theft
  - Real Estate Professionals often possess a clients personal PII (personally Identifiable Information), making identity theft that much easier. Think of how many clients a Real Estate Pro may have and the vast amount of information a hacker could steal with just one hack.

How do hackers attack Real Estate Professionals?

- Email Phishing
  - Unverified links
  - Unverified attachments
- Text message Phishing
  - Unverified links
  - Unverified attachments
- Fake social media Phishing
  - designed to fool the user into befriending the fake profile-
- Fake Ads
  - Click the link and see what happens!
- Software from unverified sources
  - Bundled software
  - Unwanted downloads
  - Apps that side load malware
- Via wireless
  - Fake cell tower

- Free wifi

- Via OS/software vulnerability
  - Oops, forgot to do those updates !

Real world attack Scenario

- Man in the middle attack
  - Using any one of the above methods to load malware
    - install packet sniffer to listen in on network communications to gain information to create fake chat service to mimic clients bank
    - Hacker creates fake website to mimic bank website
    - Hacker starts chatting with client pretending to be the bank
    - Hacker starts chat with bank pretending to the client
    - Hacker “verifies” clients credentials then passes them to bank to gain access to clients accounts.

Risk Mitigation-

- Where to start
  - The space between our ears
    - Simple rules to follow
      - DON’T CLICK ON LINKS IN EMAILS, TEXT, OR SOCIAL MEDIA
      - PHONE NUMBERS CAN BE SPOOFED- YOU CAN BE TALKED RIGHT OUT OF YOUR MONEY IN A WINK OF AN EYE- Insist calling back using the listed number of the financial institution
      - Keep every device you have updated to the latest software using trusted sources
      - Use Multi factor Authentication religiously, and use it everywhere possible.
      - Find secure method of storing passwords and change them often.

- Do not use free WiFi period unless you are using a VPN service to secure your connection.
- Keep gaming apps off of any device used for work. Most gaming apps collect way too much personal information and are often used as a Trojan to install malware.
- Keep your cell phone off when arriving or departing an overseas airport (outside the US) better yet if traveling outside the us, purchase a different phone with only the basic apps/info you need for that trip.
- If you can, remove all social media apps from your phone- too much information shared makes you an easy target!

Cell Phones

- Android vs Apple
  - Apple security better for those without IT knowledge. Since Apple controls the operating system, the apps have no access to the root coding of the operating system thus providing apple with better security up front.
  - Android “can be” more secure than apple but only with advanced knowledge to set up. Out of the box, android is far less secure than apple. It is VERY important to be careful about where android apps are downloaded from- this is androids Achilles heel. It is also suggested to use anti-virus software on android products.
- Signs your phone may be hacked
  - If your battery suddenly begins to drain quickly
  - You receive any verification texts you did NOT ask for
  - Text messages or calls appearing in your history you did not make
  - Apps appear that you did not download

Additional Comments-

- This is by no means an exhaustive list of cyber security issues. New threat vectors are being discovered every day - so many that it is difficult to keep up! The threats are coming from countries like Russia - Putin has all but legalized hacking so long as the hackers do his bidding when he asks. North Korea, Iran, China to name a

few are producing vast amount of internet traffic with just hacking alone. For some of these countries hacking is a revenue stream, for others it a way to sow division within the American people. With the introduction of quantum computing, these threats are growing almost exponentially. This is all to say that it is more important than ever to secure devices. Your financial future may well depend on it.