PROTECHt Yourself

Important tech-related information brought to you by the NDAR Cyber Alliance Committee

September 2016 Edition

Tech Article by Chris Volk

Real estate industries have not been targeted as aggressively by hackers as other industries, but real estate companies store exactly the type of personal information cyber criminals want most: social security numbers, bank account information, driver's license numbers, credit/debit card numbers. Investing in security should become a top priority. With advances in digital transactions like DocuSign it is even more important, as we move forward, to be even more cautious of what we do. People no longer have to be in your office to take information you have saved.

If your company has a website, communicates with customers via email, or stores customer information in an electronic database, you could be putting the customer at risk if you aren't taking the right precautions. Following a few simple online safety practices can protect you from incurring expensive and dangerous data breaches, and give your customers the peace of mind they deserve. The estimated cost of data stolen is between $154 to $363 per compromised record. That means if you have 100 data files of prior customers and it is compromised it could potentially cost $36,300 by that estimate. Our first job as REALTORS® is to help keep our clients confident and comfortable with us.

Gain Clients’ Trust

The following practices will help safeguard your customers' data and help them feel confident about doing business with you online.

Know what you have: You should be aware of all the personal information you have about your customers, where you're storing it, how you are using it, who has access to it and how you protect it.

Keep what you need and delete what you don't: While it's tempting to keep information for future use, the less you collect and store, the less opportunity there is for something to go wrong.

Protect what they give you: If you're holding onto information about your customers, you need to keep it secure. For instance, a California real estate investment trust reported a data breach and had to hire forensic computer experts to analyze and secure the impacted data systems. In March 2012, a Massachusetts property manager was fined $15,000 by the state because they didn’t properly secure sensitive data stored on a laptop that got stolen. The manager’s firm was also required to limit the use of portable devices and encrypt any sensitive information stored on them.

Daily Best Practices

Keeping your customers safe requires your own digital systems to be fully protected. The best policies in the world won't protect your customers if your network and resources are at risk for preventable attacks. Protecting your network and systems requires a lot of the same steps as protecting a single computer or cell phone, only on a larger scale.

Keep a clean machine: Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

Scan all new devices: Be sure to scan all USB and other devices before they are attached to the network.

Use a firewall: A good firewall keeps criminals out and sensitive data in.

Use spam filters: Spam can carry malicious software and phishing scams, some aimed directly at businesses. A good spam filter will block most of it and will make your email system safer and easier to use.

Password Security: No password is completely secure no matter how often you change it or how many special characters you add.

Use Secure Software

Never use software with a bad security track record to store or transmit sensitive information. Invest in a powerful antivirus program, and update your operating system on a regular basis. If your employees connect with their workstations remotely via laptops, smartphones, or tablets, make sure those connections are secure. VPN, Proxy Networks, or Tunneling Protocol, are easy ways to create a secure network that you can log into anywhere at any time.

Train Employees

When your employees are not properly educated on matters of data security, they can put your company at risk. Encourage staff to use caution when they browse online from their workstations. All it takes is for them to click on one harmful link, download a malicious file, or open a contaminated email, and your entire security system can be compromised. Employees should also be familiar with the basic rules for creating strong passwords.

Configure Mobile Devices for Security

Your company's data security policies should include clauses about storing sensitive information on mobile devices as well—real estate professionals are basically glued to their smartphones. Urge employees to limit installation of third party "apps" that look unreliable, protect their devices from malware, and keep their software updated. They should also use a device PIN or password and a GPS-aided phone finder, to keep sensitive data protected in case their device is stolen or misplaced.

Use Encryption

Using encryption to protect sensitive data should become common practice in the real estate world. Simply put, encryption transforms readable information into data that can only be accessed by individuals who have the right "key." Even if the data falls into the wrong hands, it can't be read.