Cyber Security for REALTORS

Disclaimer

The following are suggested practices to aid with cyber security. The problems and concerns with Internet security are constantly evolving and there is no complete solution or guarantee regarding cyber security. Southwestern Indiana Association of Realtors assumes no liability for any breach of security whether or not the guidelines are implemented. Always consult an expert.

Email Accounts

Your email account is a primary target for hackers and those with nefarious intentions. The following practices will make it more difficult for those types of attacks being successful.

1. Change your email password periodically
2. Never re-use your email password for other web sites etc.
3. Enable two-step verification. If your email or cloud service offers it. In addition to entering your password, you are also asked to enter a verification code sent via SMS to your phone.
4. Do not click on links or open attachments in email messages unless you are certain they are safe

Phishing

Phishing is defined as the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication (email).

Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern. Communications purporting to be from social web sites, auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that distribute malware.

The following are good practices to avoid becoming the victim of a phishing type email

1. Phishing emails are getting more sophisticated. They often appear to be from a legitimate source and may contain familiar logos etc. Some are more obvious to identify. Those coming from foreigners may have spelling errors or poor grammar. If in doubt, do not open attachments or click on links.
2. If you receive an unsolicited email message from a bank with a link to click on, do not click on it. Banks don't do send out solicitation messages with links.
3. If you receive and email message that appears to be from the IRS it is likely a phishing email. The IRS does not contact consumers via email.
4. If you receive an email about the status of your order (e.g. Amazon) and you have not ordered anything from that source, do not respond to, or click on any link or attachment associated with that message.
5. If you receive an email with an attachment and you do not know what the attachment is, do not attempt to open it.
6. If in doubt do not click on links or attempt to open attachments.
7. Use secure WIFI when sending and receiving email. Free, public WIFI services may not be safe.

Created 02/01/2018

It is a good practice to change your password for your email account periodically. While inconvenient, this may interrupt any nefarious activity associated with your account.

Wire Fraud

There have been many consumers that have fallen victim to wire fraud in Indiana. Hackers use a variety of methods lure victims. These include email phishing, bogus text messages and, in some cases, phone calls. One common scenario involves a hacker sending out a phishing type message to someone involved in a real estate transaction. If the recipient clicks on the link or attachment the hacker gains access to the recipient's email and is able to monitor communications without being detected. A hacker may lay dormant for any length of time. The hacker may learn who the parties and agents involved in a transaction and will intercept lender and title company information. They will witness negotiations, gain a wealth of personal information, see preliminary settlement statements and, potentially, wiring instructions. This enables them to create and send spoof communications and alternative instructions etc. Keep in mind, even if you employ safe practices, someone else in the transaction may have been hacked or otherwise infiltrated. Keep your guard up at all times.

The following are some steps to follow to minimize the risk of you or your client becoming a wire fraud victim.

1. Advise your clients to communicate directly with their lender and title company with regard to wiring instructions and to go in person or use phone numbers they are certain are correct.
2. Take yourself out of the loop. Do not receive or forward wiring instructions.
3. Tell you clients you will not send them wiring instructions
4. Exercise caution when forwarding email messages. Some messages contain a gold mine of information for hackers including a chain of correspondence with private information, and the contact information for additional parties. It is often better to initiate a new message rather than forwarding an existing message.

General Recommendations

1. Keep software, particularly your web browser up to date. Many operating systems offer automatic updates. If this option is available, you should enable it.
2. If you share your computer with other users, coworkers, family members etc. make sure the other users employ safe browsing practices.
3. Do not give sensitive information to others unless you are sure they are indeed who they claim to be and that they should have access to that information.
4. Limit the amount of personal information you share. Do not put your full date of birth on social media accounts such as Facebook.
5. Do not accept social media invitations (friend requests) from people you do not know. Do not accept a friend request if you are already "friends" with that person. The second request is likely to be a cloned account.
6. Install a reputable anti-virus solution on all computers. There are fake antivirus programs that are malware and mimic legitimate security software. Be aware of pop ups displaying unusual security warnings and seeking personal and credit card information.

Created 02/01/2018

7. Practice good password management. Change your email and other passwords periodically. Do not use the same password on multiple sites/accounts. Do not write passwords on Post-It notes and stick on your monitor or under your keyboard. Never reuse your main email password.
8. Never send credit card information or social security numbers in an email message.
9. Always shred documents that contain personal information when you no longer need them.
10. Be careful with your social media posts. Pictures taken inside your home may show valuable items. Posts about being out of town or on vacation are invitations for burglars.
11. Be careful when signing into public wireless networks. Many public hotspots do not encrypt information and therefore anything you send could be intercepted and used.
12. Avoid using public computers for banking and other ecommerce activities.
13. Only shop online on secure sites. Ensure the locked padlock or unbroken key symbol is showing in your browser. An online retailer's address will change from http to https to indicate a secure connection.