March 5, 2024

Dear King Ranch Homeowner,

It has come to my attention that members of our King Ranch community have received emails “supposedly” from my email address or from our other board member’s email addresses requesting you to supply personal information by pressing a website link on the HOA email. **I WILL NEVER NOR WILL ANY KING RANCH BOARD MEMBER EVER EMBED ANY “INFORMATION GATHERING LINK” ON AN EMAIL. OUR EMAILS ARE INFORMATIONAL ONLY AND IN SOME CASES OUR EMAILS MAY HAVE ATTACHMENTS OF PDF DOCUMENTS WHICH ARE “READ ONLY”! SUCH AS KING RANCH GOLF COURSE BULLETINS OR OUR QUARTERLY FINANCIAL REPORTS OR HOMEOWNER INVOICES.**

Our King Ranch HOA website uses internal links to different areas of the website itself. I have been extremely careful to use only valid external links on rare occasions to link to secure (SSL) outside informational website sources. My external links provided on our community website are protected, information only links. **Currently one external link exists** on our CONTACT page referencing Montana Income and Tax Rebate. I will only place valid, safe external links on the CONTACT page on our HOA website.

Again, all links on our website are “internal links” for informational purposes only.

Keep in mind "Phishing emails" are not just innocent spam. They are criminal attempts to fraudulently acquire private information from unsuspecting users such as ourselves. Some people, however, allow their greed or curiosity to get the best of them and fall for these scams. Even though some of these phishing emails are quite easy to see through, millions of people every year still fall prey to these phishing scams.

It's no secret that cybercriminals attack their targets by sending out sophisticated phishing email scams. These scams resemble emails from legitimate banks, government agencies, credit card companies, social networking sites, online payment websites, multiple online stores or in this case people we know within our community. These usually begin with an approach where the sender asks recipients to click on a link that redirects them to an ad page where they need to specify and confirm personal data, account information, etc. Worse yet many scammers are trying to access your address or contact lists on your computer when you press on a link that seemingly goes no where and then the scammer sends phishing emails from your address book to others that look like they are coming from you. All in the effort to steal money from you or someone you know. **SIMPLY**

NEVER, EVER DO IT! NEVER CLICK ON A LINK ON AN EMAIL! *CALL THE SENDER INSTEAD TO VERIFY THE EMAIL IS REAL!*

Cybercriminals or spammers—people who send spam email messages—use many different methods to collect email addresses. I have to assume since they are using our board member email addresses someone out in the internet has used a "harvesting program" to obtain board member email addresses from our website or from the State of Montana's website since those email addresses are open information and contained in various areas for referencing by the State of Montana for informational purposes.

Looking to the future I secured our website with a Secure Sockets (SSL) Certification. A secure URL should begin with "https" rather than "http." The "s" in "https" stands for secure, which indicates that the site is using a Secure Sockets Layer (SSL) Certificate. This lets you know that all your communication and data is encrypted as it passes from your browser over the internet to the website's server and back to me. ***At this time the King Ranch Website is not being used for any type of information gathering.*** The SSL was installed incase the HOA needed to use our website as a tool for homeowners to pay their dues and assessments online in the future. Remember to look for

“https” and the lock icon on any website to be sure it is safe for information exchanges.

Every King Ranch Homeowner should:

- Remember to logout of the accounts you’ve accessed before leaving the terminal, even if it’s a home computer.
- **Never open** an attachment from someone you don’t know or in many cases from someone or business you do know. No matter how tempting! EX: (Subject Line: Free Vacation! or Donate to Biden! or Donate to Trump!)
- Never share any of your PASSWORDS with anyone.
- Never upload (post) pictures of yourself or family onto the Internet or an on-line service to people you do not personally know.
- Never post vacation plans online. EX: (Facebook (META) or Instagram Status: Leaving tomorrow for a 7 day cruise! Or Family is Gone to the Frenchtown Wrestling Tournament this weekend!)
- Never post vacation pictures of you or your family online while you are on vacation. It’s an open invitation for problems if bad people are watching.
- Never download pictures from an unknown source from the internet, as there is a good chance that the picture could be contain a BOT or Harvesting program or other CODE that could effect the health of your computer or your pocket book.

- Never send money, credit card number, or account information to a non-validated source (a website without a SSL Certificate). Pay with PayPal to protect yourself!
- Make sure the intended web address you typed is correct.
- Finally NEVER, EVER freely give out identifying information such as your name, home address, school name, Social Security, Medicare, any insurance or telephone number to anyone on the internet even though the majority of this information can be found searching on the internet using Google, Bing or Yahoo. Do not give this information to unwanted calls (calls not recognized by your address book), robocalls, sweep stake winner calls, – including illegal spoofed calls.

This email is being sent to our King Ranch Community to hopefully address a problem that has been brought to my attention because of the concern about others trying to invade our privacy, collecting our private information for identity theft or for personal monetary gain. Please be internet safe! I will post this email on our website.

Craig Milam
www.kingranchhoa.org