Kerby&Cristina REAL ESTATE EXPERTS RE/MAX RESULTS

COVID-19 TOP DIGITAL SCAMS

WHAT YOU NEED TO KNOW NOW!

Beware of the following scams designed to manipulate our fears in order to steal money and compromise personal and business information.

HOW TO RECOGNIZE PHISHING, VISHING, AND SMISHING SCAMS

Keeping up with the latest news? We all may be more vulnerable to falling for fake Coronavirus update emails, texts, and voicemails. **Don't be tricked into clicking on suspicious links or sharing any personal or medical information over the phone.**

Be on the lookout for these warning signs — **DO NOT click on any links or enter any information in an email if it:**

1. Insists that you act now
2. Includes a request for personal, financial, or medical information
3. Directs you to open attachments and click on links
4. Starts off with a generic greeting and has spelling and grammatical errors throughout the message

FAKE WEBSITES

They may look legitimate, but cyberthieves are creating websites that collect your personal information and your money under the guise of providing you with:

- Coronavirus updates
- Emergency response plans
- Products: Protective face masks, sanitizers, test kits
- Investment sites for victim care

TRAVEL SCAMS

Flight and cruise deals are popping up with extreme discounts — just remember **if an offer seems too good to be true, it often is.**

- Book directly through an airline or hotel website
- Consider the company's cancellation policy before submitting payment
- Read the fine print in the travel insurance policy

SPOOFED GOVERNMENT AND HEALTH ORGANIZATION COMMUNICATIONS

Scammers disguised as government and health organizations are emailing individuals and asking a potential victim to:

- Visit a "protected" site and requiring the visitor to enter personal information to view security tips
- Open an email attachment to view detailed information that then launches a virus
- Click on a link that redirects them to a spoofed (or fake) website, asking for financial details to make donations or purchase protective products

Check the facts first:

- **Centers for Disease Control and Prevention (CDC)** https://www.cdc.gov/
- **World Health Organization (WHO)** https://www.who.int/
- **USA.gov** https://www.usa.gov/coronavirus/
- **U.S. Food and Drug Administration (FDA)** https://www.fda.gov/home
- **Federal Trade Commission (FTC)** https://www.consumer.ftc.gov/
- **U.S. Securities and Exchange Commission (SEC)** https://www.sec.gov/investor/alerts

MIRACLE CURES OR VACCINES

The Federal Trade Commission (FTC) and the U.S. Food and Drug Administration (FDA) warn:

> *" NO vaccines, pills, potions, lotions, lozenges, or other prescription or over-the-counter products available to treat or cure Coronavirus."*

FAKE JOB POSTINGS

Recruiting for "relief charities"

If you apply for a job and are asked to deposit money into your personal account, and then transfer that money to another account, you have become a "Money Mule" and are committing money laundering.

Recruiting for "crisis related medical work"

Applying to fake job listings tied to growing needs in the medical community because of COVID-19 gives thieves access to your Personally Identifiable Information (PII), such as Social Security number or bank account information.