How to Avoid Coronavirus Scams

In a time of increasing uncertainty, cybercriminals are looking to take advantage of individuals looking for information regarding COVID-19. Cybersecurity firms and the FBI are seeing an increasing number of phishing and malware scams, and expect the trend to continue as the virus spreads. With concerns over the health and safety of our loved ones and our community, it is natural instinct to let our guards down when researching information or browsing our inbox.

By now, we are all well aware of how social distancing and hand-washing can help curb the spread of the virus, but how can we help protect our digital identities?

Phishing: These scams occur when cybercriminals pose as legitimate organizations prompting you to click on fake links and attachments, asking you to enter sensitive information such as usernames and passwords. Scammers are always looking for trending subjects to capture attention and gain more clicks. With the flood of information being pushed to individuals, it is easy for phishing scams to blend in.

Criminals are now posing as the World Health Organization (WHO), Center for Disease Control (CDC), in addition to corporations, and using their branding to blend in. Recent example: emails posing to be coming from the CDC using cdc-gov.org, when the real CDC domain is cdc.gov.

Investment scams for COVID-19 cures: The SEC has reported an uptick of companies claiming they have a cure for the outbreak and seeking investment. These are typically microcap stocks looking to increase the price significantly quickly then have the promoters dump their shares and run off with the profits.

Links to watch out for: Cybersecurity company, Recorded Future, specifically called out the following domains as dangerous:

- coronavirusstatus.space
- coronavirus-map.com
- blogcoronacl.canalcero.digital
- coronavirus.zone
- coronavirus-realtime.com
- coronavirus.app
- bgvfr.coronavirusaware.xyz
- coronavirusaware.xyz
- corona-virus.healthcare
- survivecoronavirus.org
- vaccine-coronavirus.com
- coronavirus.cc
- bestcoronavirusprotect.tk
- coronavirusupdate.tk

- Treat all COVID-19 outbreak emails with caution: Scammers will often use fear and urgency tactics in order to get you to click or open attachments.
- Think before you click: If an email asks you to click on a link, always try to find another way to validate it such as reaching out via a phone call.

- Analyze URLs and email addresses carefully.
- Wrong addresses and misspelled domains are common red flags.
- Use anti-virus tools and turn on auto-updates for all of your devices.
- If something sounds too good to be true, it probably is. If you come across any investment scams or securities fraud, report to https://www.sec.gov/tcr.

We know these times feel uncertain. If you have questions regarding your investment strategy or financial plan, please reach out to your Wealth Consultant. If you are not a current Evergreen client, please email info@evergreengavekal.com to be connected to one of our trusted advisors who will review your comprehensive financial picture and make recommendations for an investment strategy in these volatile times.