Scam Watch

Like the rest of us, con artists have plenty of time on their hands these days. And the growing number of hours spent at the computer (or phone) mean there are more victims. Protect yourself by watching out for these ripoffs:

COVID-19 concerns. It's an understatement to say that COVID-19 has launched countless scams in the form of phishing emails, phony phone calls, bogus "cures," and more. In just the first few months of the coronavirus era, U.S. consumers reported $12 million in pandemic-related ripoffs. At a time like this, it's critical that you remain skeptical, hone your ability to spot phishing emails, and never click unverified links.

'Fearware' fever. The first specific coronavirus scam we'll point to, as it has sucked in many victims already, has been dubbed "fearware." This attack may be an expertly crafted phishing attack, or it may be a map purporting to show cases in your area—in either case, it actually downloads malware to your device. The fraudsters know that with COVID-19 on everybody's mind, people are more likely to click where they shouldn't.

Router ripoff. A new hack of home and small-office routers is redirecting users to malicious sites that pose as COVID-19 informational resources in an attempt to install malware that steals passwords and cryptocurrency credentials, Bitdefender says. Popular routers from Linksys and D-Link have been targeted, though it remains unclear how attackers are compromising them. Researchers suspect hackers are guessing passwords—so change yours ASAP!

Stimulus stupidity. Well *that* didn't take long: with the federal government getting set to send most Americans a check, researchers say crooks are already phoning, texting, and emailing people telling them they have to make an upfront payment to release their entitlement. Not so! If you're asked to pay, this is absolutely, positively a scam.