**R U Ready?**

***A major Russian Cyber attack has been forecasted. If it happens, it will be very disruptive, and people who are not prepared, are likely to suffer immensely.***

What can you do to be ready to deal with life threatening changes that will seriously impact the lives of the many who are unprepared. What can we expect if a major cyber attack does happen? A major cyber attack from the Russians, or any other significant entity, will impact four major targets: energy, water and electrical infrastructure, and financial institutions, cloud-data companies and telecommunications firms. A successful, or partially successful attack may cause major disruptions to normal life in our country, that may last hours, days, or weeks. What should we do, to prepare for that major disruption of life?

1. Stock up on non-perishable foods (don’t forget a working can opener) and one gallon of fresh water per person, per day. Get a windup emergency radio, a portable power station and USB ports to keep your cell phone functioning.
2. Save 2 weeks of cash in small bills (1, 5 and 10 dollar bills) as the places you need to spend money may not have change. ATMs may not be available when you need them, thus we all need an emergency funds.
3. Back-up your essential personal information, including passwords to your banks and other financial institutions. Be sure to store important papers, photos and important personal documents a portable hard drive, in the cloud, and in memory sticks. Maintain at least 2 weeks of necessary medications available.
4. Hackers globally will likely exploit our vulnerable time to scam you with phishing emails, so don’t give them any help to enrich their pocketbooks. Seniors will likely be a major target for scammers. Help protect your family senior members who use computers to protect them from scammers.
5. Keeping your families together if at all possible. If family members are spread out, arrange for a single location to gather after 2 4 hours.
6. Maintain multiple lines of communications, including landline phones which may not be as vulnerable as cell phones and other wireless equipment.
7. A simple device that can be very valuable can be a small notebook, to maintain all your passwords, the addresses of all you family and key friends, and other important data you use everyday, which may be even more important under a cyber attack.
8. There may be other important issues of unique importance to any individual or family. Think about these matters now so that you can be prepared.
9. Regarding our cars, always keep the gas tanks in your cars at least half full so that you can re-locate to a better location.

It is not possible to list everything, everyone needs to do in case of a major disruption to our lives, so think ahead and plan ahead. We can hope that it won't happen, but what would you do it does happen.

Best of luck to everyone.

===================================================

**SOURCES:**

***https://www.popsci.com/technology/russian-cyberattack-concerns/***

“**Are you prepared for a Russian Cyberattack**?”, Jon Sileo, BottomLine, June 15, 2022 p 1-3.

**Shira Feder covers tech, science, and health. She holds a master’s degree from the Craig Newmark Graduate School of Journalism and has written for The Washington Post, Vox, The Daily Beast, Business Insider, and other publications.**

**How worried should we be about Russian cyberattacks?**

**Experts differ on the threat level, although there are common-sense steps that people, organizations, and governments can take to protect themselves.**

In the wake of Russia’s invasion of Ukraine, it makes sense to wonder: Should America be worried about cyber attacks right now? Experts have mixed opinions.

One way to gauge what potential Russian attacks could look like is to analyze past events. “We know from what Russia has done in the past, what they’re capable of,” says Glenn Gerstell, former General Counsel of the United States National Security Agency from 2015 to 2020. “And they’ve used Ukraine as a little bit of their cyber punching bag, so to speak.”

Since 2015, when a Russian attack took out Ukraine’s electrical grid, Ukraine has worked hard to shore up its digital defenses. But in 2017, NotPetya, a Russian cyber attack against Ukraine that spread around the world, still caused billions in damages. There was also the 2021 Solar Winds attack, which targeted American companies like Microsoft and Intel, as well as various American federal agencies, including the Pentagon, the Department of Homeland Security, and the National Nuclear Security Administration, leaving them exposed.

Now, with America imposing sanctions on Russia, many fear a retaliatory attack. Here’s what you need to know about the topic.

**What kind of attacks has Russia delivered in the past?**

First, keep in mind the time period. “It’s important not to fall into a Cold War mindset and think about cyber attacks like an episode of Stranger Things, where spies are popping out of the sewers,” says privacy researcher Sean O’Brien, who leads Yale’s Privacy Lab. According to O’Brien, attributing cyber attacks to a whole country, or even a specific group within that country, is difficult. Plus, adversaries can pretend to be someone else, in ways specifically designed to obfuscate their nationalities.

But we do know that historically, Russia has tested out some of its most destabilizing cyber attacks on Ukraine, and have shown they have access to water and power systems there. Some of the different strategies they use to destabilize systems include DDoS attacks, where an attacker sends large amounts of traffic to a website and essentially overwhelms it with more requests than it can handle. They also use wiper attacks, designed to wipe all the data in a given network, and hack Ukrainian national security sites for the purpose of getting intelligence about that country.

[Related: Cybersecurity experts say $2 billion is too little, too late]

In January 2022, Microsoft disclosed that there was a malware attack on the Ukrainian government. There have also been a spate of recent hacks that may or may not have been Russian. During the first week of the invasion, hackers leaked proprietary data from US microchip dynamo Nvidia online, leading some to wonder if the attack was tied to Russia. In February, hackers gained access to 21 major energy companies in America, including Chevron and Kinder Morgan. This operation was discovered on the eve of Russia’s attack on Ukraine, again causing speculation about its source.

Jason Leigh, a special agent on the FBI Houston’s cyber task force, told Bloomberg that he expects that the Russian hacking invasions “may escalate in terms of volume or the number of attacks and the manners in which they attack.”

Should people be worried about Russian cyberattacks right now?

When the Ukraine invasion first occurred, some felt cyberattacks were inevitable, and the US Department of Homeland Security warned businesses to be on alert for Russian cyberattacks. But so far, nothing has happened—that we know about.

Data breach hunter Chris Vickery says if the Russians had the power to enforce their will via cyber means, America would already have been attacked. “If Russia had the capability to be invincible online cyber warriors, they would have done something already,” he argues.

Gerstell, formerly of the United States National Security Agency, disagrees with this notion, pointing out that precision cyber attacks, the kind that are used to take down electric grids and petroleum refineries, take time to plan. “The bottom line is America is still vulnerable,” he says. “We’ve got everything from the retail sector to other big pieces of critical infrastructure that are in varying states of vulnerability. Putin has the capability. And all that’s missing in that equation right now is the strategic decision to exploit that vulnerability.”

Gerstell adds that Putin may not have expected such a strong response from America, with sanctions that have devalued the ruble.

Some American companies are also offering free cybersecurity services to both Americans and Ukrainians, like cybersecurity intelligence company GreyNoise, which automatically upgraded all Ukrainian email accounts to include full access to its products. Tesla announced they will continue paying Ukrainian employees if they have to travel back home to help the military for up to three months. Elon Musk, Tesla’s CEO, sent out Starlink equipment to Ukraine, which could enable voice calling and Internet access if the Internet was otherwise unavailable, although some have pointed out that these satellites could put the country at further risk.

Currently, Putin has a lot to lose and little to gain from launching a cyber attack, Gerstell says, but if he feels cornered, that could potentially change his course of action.

**How can we protect ourselves?**

If you haven’t already, turn on multi-factor authentication and back your stuff up, says Vickery, a self-described data breach hunter. Companies should keep track of who their contractors and subcontractors are, and lock down IP addresses that are not in their systems. “If governments nationwide did all those things, we would be in very, very good shape,” he says.

Anne Neuberger, who serves as the Deputy National Security Advisor for Cyber and Emerging Technology in the Biden Administration, offered her advice on a New York Times podcast. “For data that’s most important to you, your bank records, your health records, keep a backup copy that’s disconnected from the internet so that in case something happens, you have that available,” she said.

Gerstell’s recommendation involves backing up data, ensuring antivirus programs are up to date, checking computer logs more frequently, and patching everything you’re capable of patching. “Long term, you could really change the architecture of the systems that you have to be far less vulnerable, and that probably means moving to something called zero trust architecture,” he says, explaining that zero trust architecture is a strategic approach that continually validates every stage of online interaction.

Are there international laws establishing cyber policies?

Yes. The Budapest Convention on Cybercrime, which was established in 2001, was the first international treaty to try coordinating cyber crime responses across nations. The UN Group of Governmental Experts’s goal is to establish “responsible state behavior in cyberspace in the context of international security.” They’ve outlined a set of voluntary policies for cyber use, which include not attacking crucial online infrastructure.

In the United States, one common complaint is the lack of a cohesive response for handling cyber crime across state governments and the federal government, leaving individual departments to make crucial decisions without sharing strategic intelligence. Chris Inglis, the first National Cyber Director, echoed these complaints, writing that America needs a centralizing response that “meaningfully alters the relationship between public and private sectors.”

**So what happens now?**

We’ve got to start playing catch-up, experts say. “For 20 years we’ve been enjoying the benefits of unimaginable innovation on the internet,” Gerstell says. “We’ve been so focused on this intoxicating, dizzying array of wonderful, wonderful benefits and functionality that we haven’t spent a fraction of the energy and time on the defensive side and that’s now catching up.”

The good news? Solving the country’s cybersecurity problem is not exactly a mystery. We know how to make networks safe, but it’s difficult, expensive, and time-consuming. “But we could do it,” says Gerstell. “So that’s the challenge.”