SHIELDS UP

While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia's unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity.

You can avoid cyber risks by taking steps in advance:

- **Limit the personal information you share online. Change** privacy settings and do not use location features.
- **Keep software applications and operating systems up to date.**
- **Create strong passwords** by using upper and lower case letters, numbers, and special characters. Use a password manager and two methods of verification.
- **Watch for suspicious activity** that asks you to do something right away, offers something that sounds too good to be true or needs your personal information. Think before you click. When in doubt, do NOT click.
- **Protect your home and/or business using a secure Internet connection** and Wi-Fi network, and change passwords regularly.
- **Don't share PINs or passwords.** Use devices that use biometric scans when possible (e.g., fingerprint scanner or facial recognition).
- **Check your account statements and credit reports regularly.**
- **Be cautious about sharing personal financial information,** such as your bank account number, social security number, or credit card number. Only share personal information on secure sites that begin with https://. Do not use sites with invalid certificates. Use a Virtual Private Network (VPN) that creates a more secure connection.
- **Use antivirus and anti-malware solutions and firewalls to block threats.**
- **Back up your files regularly in an encrypted file** or encrypted file storage device.
- **Do not click on links in texts or emails** from people you don't know. Scammers can create fake links to websites.
- **Remember that the government will not call, text or contact you via social media** about owing money or receiving economic impact payments.
- Keep in mind that **scammers may try to take advantage of financial fears** by calling with work-from-home opportunities, debt consolidation offers, and student loan repayment plans.

During a Cyberattack

- **Check your credit statement** for unrecognizable charges.
- **Check your credit reports** for any new accounts or loans you didn't open.

- **Be alert for soliciting emails and social media** users asking for private information.
- If you notice strange activity, **limit the damage by immediately changing all of your internet account passwords.**
- **Consider turning off the device.** Take it to a professional to scan for potential viruses and remove any that they find. Remember: A company will not call you and ask for control of your computer to fix it. This is a common scam.
- **Let work, school or other system owners know.**
- **Run a security scan on your device** to make sure your system is not infected or acting more slowly or inefficiently.
- **If you find a problem, disconnect your device from the Internet** and perform a full system restore.

After a Cyberattack

Let the proper federal, state and local authorities know if you believe you have been a victim of a cyberattack.

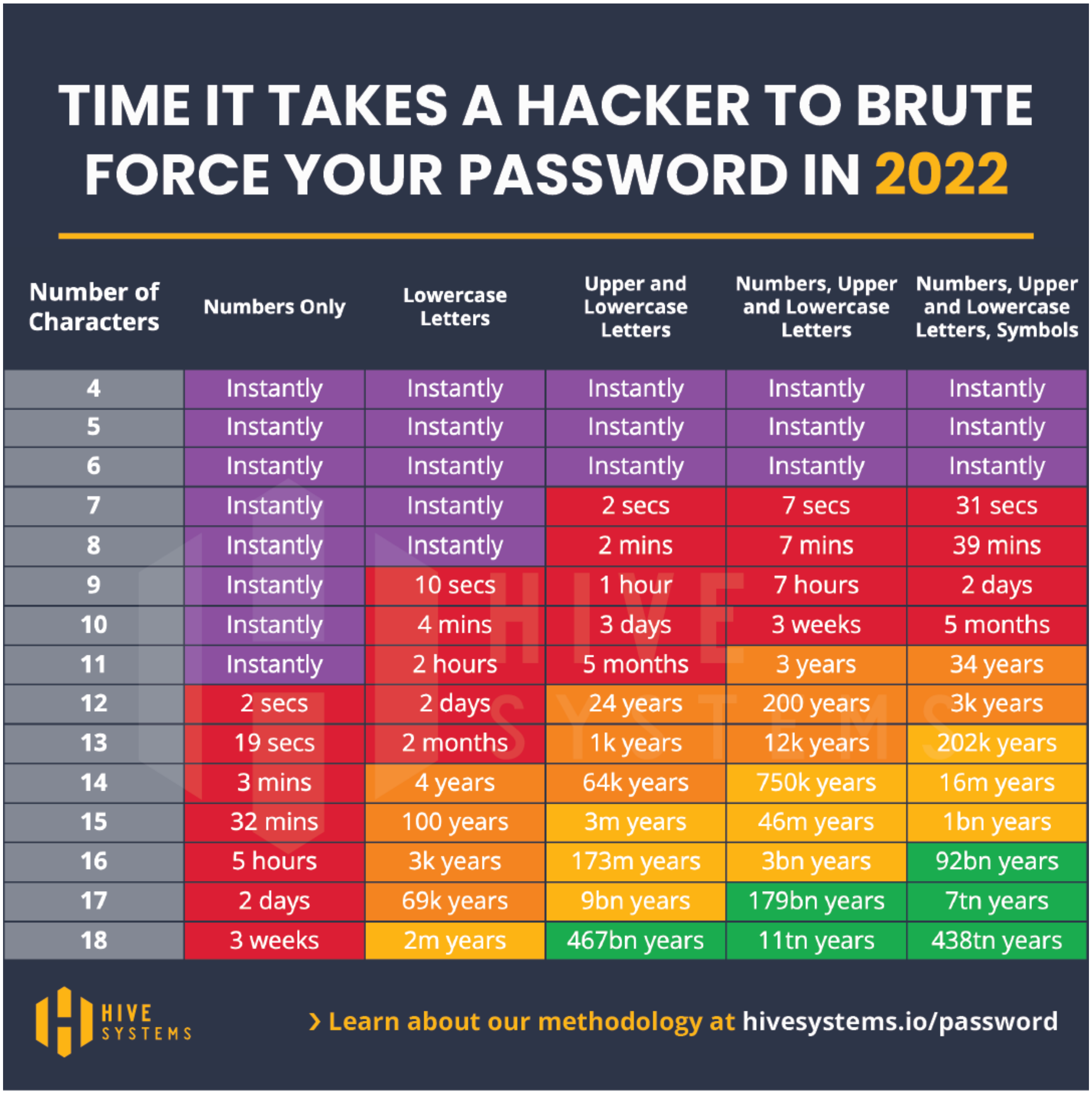
- **Contact banks, credit card companies and other financial services companies** where you hold accounts. You may need to place holds on accounts that have been attacked. Close any unauthorized credit or charge accounts. Report that someone may be using your identity.
- **File a report with the Office of the Inspector General (OIG)** if you think someone is illegally using your Social Security number.
- **File a complaint with the FBI Internet Crime Complaint Center (IC3).** They will review the complaint and refer it to the appropriate agency.
- **File a report with the local police** so there is an official record of the incident.
- **Report identity theft** to the Federal Trade Commission.(ftc.gov)
- **Contact the Federal Trade Commission** (FTC) at ftc.gov/complaint if you receive messages from anyone claiming to be a government agent.
- **Contact additional agencies depending on what information was stolen**. Examples include contacting:
    - The Social Security Administration (800-269- 0271) if your social security number was compromised, or
    - The Department of Motor Vehicles if your driver's license or car registration has been stolen.

- **Report online crime or fraud** to your local United States Secret Service (USSS) Electronic Crimes Task Force or the Internet Crime Complaint Center

Thank you to Ready.gov and CISA.gov for this information!

Thanks to The Cybersecurity & Infrastructure Security Agency (CISA.gov) for this information!

Are All Your Passwords in the Green?



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

> Learn about our methodology at hivesystems.io/password

https://www.hivesystems.io/password

These metrics assume you're using a password that has not been part of a breach in the past. Attackers will try hashes to all common and breached passwords before bothering to crack new ones. (In the context of passwords, a "hash" is a scrambled version of text that is reproducible if you know what hash software was used)

- Check to see if any of your passwords, email addresses or phone numbers have been compromised: https://haveibeenpwned.com/
  If your bank or any other internet connected account only requires or allows less that the metrics for "Yellow" or "Green," enable two-factor authentication to help keep your account and information secure.
- BE SAFER -Two-Factor authentication should be enabled wherever it is offered.