Ulliance 25TH

Enhancing People. Improving Business.

August 21, 2019

Wellness Wednesday

What To Do If Your Email, Passwords Or Bank Info Were Stolen

You probably get monthly updates from your credit card company, as well as through sites like Credit Karma. And while you might not pay a whole lot of attention to alerts about that credit card you opened recently or tiny changes to your credit score, there's one message that's sure to stop you from scrolling past: Your personal information was found on the dark web.

Say what? If you've heard anything about the dark web, you know that can't be a good thing. But what does it actually mean when your information is exposed to the dark web — and what can you do about it? Here's what you need to know:

What is the "dark web," exactly?

If you imagine the internet as an iceberg, the visible part peeking above the water is the internet as we know it, explained Ana Bera, co-founder of home security website safeatlast.co. However, there's much more to it. "The part of the iceberg we don't get to see holds an enormous part of the web," Bera said. In fact, up to 90% of the whole internet is considered to be the "deep web." Though it sounds ominous, the deep web is simply the parts of the internet that aren't indexed by search engines such as Google, and therefore, don't show up in search results pages. "The deep web is usually benign and it's filled with private databases not meant to be shared with the public," Bera said.

For example, your Amazon account pages and online banking platform are all parts of the deep web. The dark web, on the other hand, is more sinister. Bera explained that the dark web is a small section of the internet that people often use to stay anonymous. Not just anyone can hop onto the dark web and start browsing; the content here exists on an encrypted network and requires certain software and authorization to access. Most websites that operate on the dark web use the Tor encryption tool, which much like a VPN, hides users' IP address and location.

"It can be used by whistleblowers, by the intelligence community to protect their online communication and by 'regular' people who wish to hide their data from marketers and websites," she said. However, thanks to the anonymity that the dark web provides, it's also a hotbed of criminal activity, where people can buy and sell drugs, weapons, and more.

"There are identity thieves that use the dark web to buy and sell people's personal information," said Patricia Vercillo, vice president of operations at The Smith Investigation Agency, a private investigations firm. "If you've ever been hacked in the past, I can assure that the dark web is most likely where your personal information is currently living."

According to Experian, that information can go for quite a bit of money, depending on what it is. For example, Social Security numbers sell for $1 each, while debit or credit card numbers can cost as much as $110. One of the most valuable items is a "Fullz," a bundle of information that includes a victim's name, Social Security number, birth date and account numbers, which can be used to inflict a lot of damage right away. Passports and medical records can sell for $1,000 or more, depending on the completeness of the information and whether it's a single entry or entire database.

But how do these criminals get their hands on your information in the first place?

Sometimes, it's as simple as leaving mail and other documents with sensitive information in the trash for someone to find. Other times, it's due to a data breach that you have no control over. And sometimes, it can be weak Wi-Fi networks and online security. If you're browsing an unencrypted website, for example, hackers can stage a 'man-in-the-middle' attack, according to Vercillo. This involves intercepting communications and pulling information from your exchanges with another person or website. "Just think about all the information you currently share online on the regular," she said. Regardless of how your data was accessed, or whether or not it was your fault, there's a good chance that something is floating around the dark web, waiting for the right buyer.

What to do if your info is found on the dark web

If you receive a notification from your credit monitoring service that your information was found on the dark web, you might wonder what you can do about it. Unfortunately, the answer is not much. After all, you can't call up the head of the dark web and ask that your information kindly be removed. Even so, there are a few precautionary measures you can take to make it harder for identity thieves to access your information, or use it if they already have it.

AVOID PUBLIC WIFI NETWORKS: You might be tempted to hop on the WiFi at your local coffee shop or hotel to save cell phone data, but Vercillo says you should think twice. "This is where hackers can easily place themselves and intercept online traffic," she said. Even password-protected networks are vulnerable to hacking. If you must use the public Wi-Fi, avoid accessing any important information or accounts.

USE A PASSWORD MANAGER: One of the simplest ways to protect your personal information is by using a unique, complex password for every account and changing it regularly. But this is an area where we tend to get lazy. Think about it: How many of your accounts have the exact same password that you've been using for years? Lancaster suggested using a password manager to simplify the process. These tools, many of which require a low monthly fee to use, create complex passwords for every account you own and store them all so you don't have to remember what they are. Just don't lose the master password to your manager.

USE TWO-FACTOR AUTHENTICATION: If someone does get their hands on the password to your email or bank account, using an additional security step can prevent them from actually getting in. "People should make sure they've enabled two-step authentication on all online accounts," Bera said. This means that when you attempt to login to an account, an additional step such as entering a code sent to your phone or verifying your identity with a fingerprint is also needed. In this case, a password alone isn't enough to get into the account.

MONITOR YOUR CREDIT: Even if you're super careful about protecting your personal information, data breaches are, unfortunately, an unavoidable reality these days. That means you have to be proactive about protecting your information and credit. "Most people hear about a breach here and breach there and just think, 'It happens, I'm too small to be worried about that. No one really wants to get anything from me,'" said Kevin Lancaster, co-founder and CEO of dark web monitoring company ID Agent. The truth is that every bit of information has a price tag. Signing up for credit monitoring and regularly checking your credit reports will help you catch identity theft early, before too much damage has been done.

FREEZE YOUR CREDIT: If you believe your personal information has been compromised, Vercillo recommends placing a freeze on your credit. A credit freeze, which is free to set up and remove, prevents lenders from pulling your credit file until they've taken an extra step to verify your identity first. This prevents others from opening new accounts in your name (though it doesn't stop someone from using an existing account, such as a credit card). To place a credit freeze, you need to contact each credit bureau individually. And you may want to consider freezing your child's credit while you're at it. Article source: http://bit.ly/2ZgbqTB

This Week's Exercise

PLIE DUMBBELL SQUAT

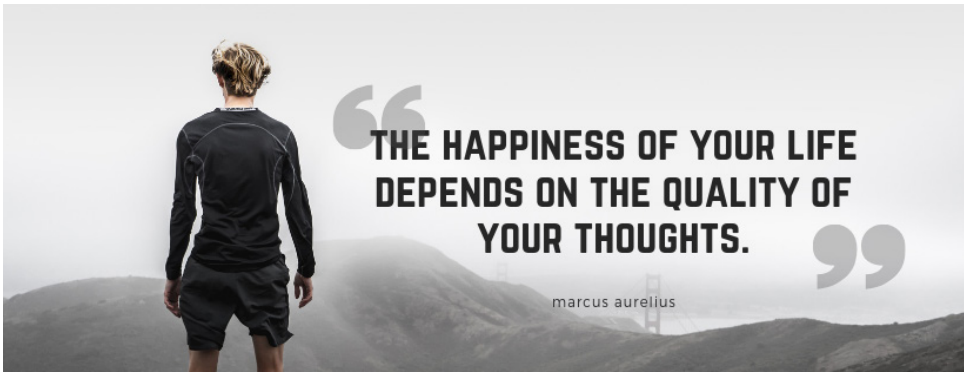
HOW TO DO IT:

1. Hold a dumbbell at the base with both hands and stand straight up. Move your legs so they are wider than shoulder-width apart from each other with your knees slightly bent.
2. Your toes should be facing out.
   Note: Arms should be stationary while performing the exercise. This is the starting position.
3. Slowly bend the knees and lower your legs until your thighs are parallel to the floor.
   Make sure to inhale as this is the eccentric part of the exercise.
4. Press with the heel of the foot to bring the body back to the starting position while exhaling.
5. Repeat for the recommended amount of repetitions.

Caution: Failure to keep your back straight can result in back injury.

Source: https://bbcom.me/2Zf0LIT

Regular exercise can help you control your weight, reduce your risk of heart disease, and strengthen your bones and muscles. But if it's been awhile since you've exercised and you have health issues or concerns, it's a good idea to talk to your doctor before starting a new exercise routine.



ARROZ CONGRI (CUBAN RICE AND BLACK BEANS)

Ingredients

2 tsp olive oil
1/2 cup chopped green bell pepper, chopped
1/2 cup chopped red bell pepper, chopped
small onion, chopped
2 cloves garlic, minced
1 cup uncooked long grain rice
15 oz can black beans (don't drain)
1 1/2 cups water
1/2 tsp cumin
1 bay leaf
pinch oregano
salt and pepper to taste

Directions

1. In a heavy medium sized pot, heat oil on medium heat.

2. Add onions, peppers and garlic and saute until soft, about 4-5 minutes.

3. Add rice, beans, water, cumin, bay leaf, oregano and salt and pepper. Simmer on medium-low heat, stirring occasionally, until the rice absorbs most of the water and just barely skims the top of the rice.

4. Cover, reduce heat to low, and simmer 20 minute (don't peek).

5. Make sure you have a good seal on your cover, the steam cooks the rice. After 20 minutes, shut flame off and let it sit, covered another 5 minutes (don't open the lid).

Nutrition Information

Serving: 1cup
Calories: 143kcal
Carbohydrates: 27.5g
Protein: 6.5g
Fat: 2.5g
Saturated Fat: 0.5g
Sodium: 322mg
Fiber: 5g
Sugar: 2g
Freestyle Points: 4
Points +: 4

Recipe source:
http://bit.ly/2Zg4mGK