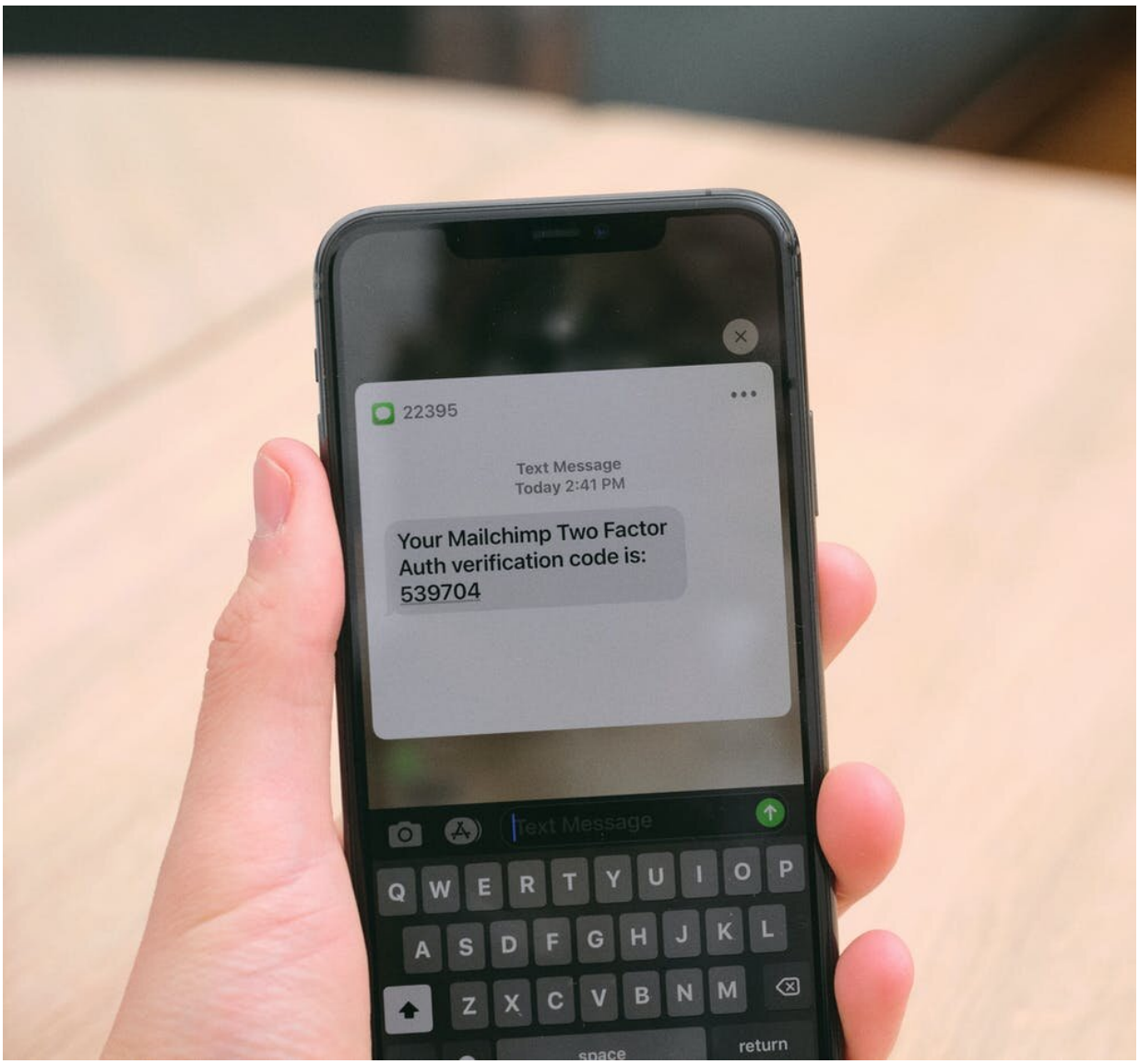
Ransomware, data breach, cyberattack: What do they have to do with your personal information?

June 24 2021, by Merrill Warkentin



Two-factor authentication, which typically involves receiving a code in a text message, provides an extra layer of security in case your password is stolen. Credit: The Focal Project/Flickr, CC BY-NC

The headlines are filled with news about ransomware attacks tying up organizations large and small, data breaches at major brand-name companies and cyberattacks by shadowy hackers associated with Russia, China and North Korea. Are these threats to your personal information?

If it's a ransomware attack on a pipeline company, probably not. If it's a hack by foreign agents of a government agency, maybe, particularly if you're a government employee. If it's a data breach at a credit bureau, social media company or major retailer, very likely.

The bottom line is that your online data is not safe. Every week a new major data breach is reported, and most Americans have experienced some form of data theft. And it could hurt you. What should you do?

Mildly annoyed or majorly aggrieved

First, was the latest digital crime a ransomware attack or was it a data breach? Ransomware attacks encrypt, or lock up, your programs or data files, but your data is usually not exposed, so you probably have nothing to worry about. If the target is a company whose services you use, you might be inconvenienced while the company is out of commission.

If it was a data breach, find out if your information has been exposed. You may have been notified that your personal data was exposed. U.S. laws require companies to tell you if your data was stolen. But you can also check for yourself at haveibeenpwned.com.

A data breach could include theft of your online credentials: your user name and password. But hackers might also steal your bank account or credit card numbers or other sensitive or protected information, such as your personal health information, your email address, phone number, street address or Social Security number.

Having your data stolen from a company can be scary, but it is also an opportunity to take stock and apply some common-sense measures to protect your data elsewhere. Even if your data has not been exposed yet, why not take the time now to protect yourself?

How bad is it?

As a cybersecurity scholar, I suggest that you make a risk assessment. Ask yourself some simple questions, then take some precautions.

If you know your data was stolen, the most important question is what kind of data was stolen. Data thieves, just like car thieves, want to steal something valuable. Consider how attractive the data might be to someone else. Was it highly sensitive data that could harm you if it were in the wrong hands, like financial account records? Or was it data that couldn't really cause you any problems if someone got hold of it? What information is your worst-case vulnerability if it were stolen? What could happen if data thieves take it?

Many e-commerce sites retain your purchase history, but not your credit card number, so ask yourself, did I authorize them to keep it on file? If you make recurring purchases from the site, such as at hotel chains, airlines and grocery stores, the answer is probably yes. Thieves don't care about your seat preferences. They want to steal your credit card info or your loyalty rewards to sell on the black market.

What to do

If you haven't already, set up two-factor authentication with all websites that store your valuable data. If data thieves stole your password, but you use two-factor authentication, then they can't use your password to access your account.

It takes a little effort to enter that single-use code sent to your phone each time, but it does protect you from harm when the inevitable breach occurs. Even better, use an authentication app rather than texting for two-factor authentication. This is especially critical for your bank and brokerage accounts. If you think your health-related information is valuable or sensitive, you should also take extra precautions with your health care provider's website, your insurance company and your pharmacy.

If you used a unique password instead of reusing a favorite password you've used elsewhere, hackers can't successfully use your credentials to access your other accounts. One-third of users are vulnerable because they use the same password for every account.

Take this opportunity to change your passwords, especially at banks, brokerages and any site that retains your credit card number. You can record your unique passwords on a piece of paper hidden at home or in an encrypted file you keep in the cloud. Or you can download and install a good password manager. Password managers encrypt passwords on your devices before they're sent into the cloud, so your passwords are protected even if the password manager company is hacked.

If your credit card number was exposed, you should notify your bank. Now is a good time to set up mobile banking alerts to receive notifications of unusual activity, big purchases and so on. Your bank may want to issue new cards with new numbers to you. That's

considerably less of a hassle than experiencing identity theft.

You should also consider closing old unused accounts so that the information associated with them is no longer available. Do you have a loyalty account with a hotel chain, restaurant or airline that you haven't used in years and won't use again? Close it. If you have a credit card with that company, make sure they report the account closure to the credit reporting agencies.

Now is a great time to check your credit reports from all three credit bureaus. Do you rarely apply for new credit and want to protect your identity? If so, freeze your credit. Make sure to generate unique passwords and record them at home in case you need to unfreeze your credit later to apply for a loan. This will help protect you from some of the worst consequences of identity theft.

Provided by The Conversation