Staying Safe Doesn't Get Any Easier

Physhing, Revisited

Forgiveness please for being repetitive here but this seems important, The initial physhing scam article appeared in this space in August, 2023. Since then, a number of things have happened to make the problem more of a threat and easier for those without souls to do their filthy work.

While there are *many* different types of scams, the one commonality is that contact has to be established between the scammer and the victim.

Some, perhaps many, of us in the neighborhood received recent notifications that our information was seen by cybercriminals. Some of this involved medical information and personal data. The number of records illegally obtained is listed as a "substantial number of Americans."

Here's part of an actual notice received via the USPS.

CHANGE
HEALTHCARE
P.O. Box 989728
West Sacramento, CA 95798-9728

To enroll in free credit monitoring services, please visit:
www.changecybersupport.com and click the link to register online with IDX.

September 3, 2024

2181636:501A A 6363
[redacted]

Notice of Data Breach

To [redacted]

We are sorry to tell you about a privacy event. This letter is from Change Healthcare ("CHC"). We work with many doctors, health insurance plans, and other health companies to help provide health services or benefits. This event may have involved your data.

What happened?
On February 21, 2024, CHC found activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began investigating right away and hired a special team to

Another breach by National Public Data (NPD) virtually guaranteed that every American's social security number is in the hands of criminals. Reportedly, some of this information was up for sale on the dark web for $3.5 million dollars.

So, even if you've not received notification, consider yourself a more likely target than you were before.

OK, while this is distressing, it's not cause for panic. But it is another reason to be more cautious than ever. Steps to take when you get a breach notification is to understand what's happening.

Often a company that has experienced a breach will offer free credit monitoring service for a period of time. If this service is ever offered, you should accept. You might also consider freezing your credit and instituting a fraud alert. Not difficult. You'll find instructions on how to do this by googling *credit freeze*. There are a number of YouTube Videos that describe the process in detail.

So, why is this article titled ***Physhing Revisited***? Think of what Physhing is. It is really mining data for possible victims. Now that the scammers have struck the mother lode, one can expect the number of attacks to increase dramatically.

One can assume that these physhing scams will increase in frequency and sophistication. Attacks detailing "undeliverable packages" or the mythical "Paypal Payment" or the "prize" you've just won will probably become more detailed and precise. The term ***Spear Physhing*** is appropriate here. Physhing is usually broadcast using a wide net. Spear Physhing uses specific user information to convince the recipient that the sender is legitimate.

An online article, https://tech.co/news/data-breaches-updated-list gives some detail on what's been happening this year. Recommended reading.

Suspicion and distrust are not usually good traits but in the case of protecting your online security, they are valuable tools.

And remember. Don't talk to strangers!

Any Comments, clarifications or questions should be directed to the author at jgf6217@gmail.com.
Written by Joe Fitzpatrick