Staying Safe Doesn't Get Any Easier

Nothing New – Let's revisit some of the ever present on line and phone threats that, having been around a while, continue to grow even more. Here's a short review of two of them.

Phishing – Like what it was named for, it casts a wide net, generating millions of emails, texts, and social media contacts without any real idea of its target. But, like successful salesmen say, "Knock on enough doors.." You get the point. And if "knocking on ten million doors" is easy, why not? How many hits do you need to drain a few savings accounts?

Spear Phishing – Any of us who have attempted spear *fishing* know that the target must be seen to be attacked. So spear *phishing* is related in that the target must be identified and targeted somewhat more precisely. So the scam artists have acquired some knowledge about you. Maybe they've gained some insight regarding your on line habits or maybe they've hacked a database with your information in it. But when you, a Jewish person, gets persuasive interactions on WhatsApp from what looks like another Jewish person, it gives you pause. It looks legitimate, perhaps associated with a group to which you belong. This is spear phishing at its best (or worst).

So, Why Are These Attacks Increasing? Because they work. And because the technological tools available are increasingly clever and we, the targets, are sometimes easy prey. An example of this is the use of Artificial Intelligence (AI) tools. The author can attest that these tools, often free, are really good at repetitive tasks, e.g. program coding and data mining. Now, using these tools to perform illegal activities reduces the work load for scammers as well, enabling them to increase their output, perhaps exponentially.

And while you may have been careful guarding your information, others that have access to it may not have been so careful, e.g. your medical care provider.

Something New – We are notified of data breaches by affected firms. Recently, some of us received a notice via the USPS regarding our medical records being compromised. The breach was real and we were offered credit monitoring for two years. Now scammers, innovative if not quite human, have been sending notices that mention data breaches and remediation requirements. Whew. This gets hard. But the bottom line is, when personal information is requested, it's a scam. The fact that scammers are paying for postage to perpetrate these crimes shows a certain confidence in their expected return rate.

And Another Something New – And this really does get wearying. But it needs mentioning. The majority of us have had our credit card hacked at some point. It's inconvenient, especially while traveling, but it's usually resolved quickly when you check your credit card usage, *which everyone should do regularly.* You call the 800 no. on your card, they take care of it, reverse the charges and maybe issue a new card. But now, *wait for it*, "Visa" has started calling cardholders to warn of fraud on your account and of course asking you to verify your info. **NO, NO, NO!** They don't do that. Hang up and call the 800 no. on your card.

And remember. **Don't talk to strangers!**

Any comments, clarifications or questions should be directed to the author at jgf6217@gmail.com