Self-Reliance Institute Newsletter

February 2015 Volume 3, Issue 02

These Red Flags Signal Dangerous Email

In an advisory that I sent you at the end of December, I wrote about the need for all of us to sharpen our ability to spot phishing emails.

You'll recall that a phishing email is a scam in which the cybercriminal sends out legitimate-looking email in an attempt to steal personal and financial information from victims. Typically, the emails appear to come from well-known and trustworthy websites but are fraudulent.

In all my years as a private detective and information security consultant, I've never seen as many phishing scams underway as there are today.

It's an epidemic.

So, in my quest to keep as many people as well-informed as possible about the dangers of phishing emails and how to spot them, I came across a good poster that lists many of the red flags of social engineering.

What is social engineering? Well, in the context of phishing emails, it can be defined as the art of manip-

Phishing continued page 6

IN THIS ISSUE

Potential Attacks on Critical Infrastructure

If 2014 was the year of data breaches, it is quite possible that 2015 will be the year that we start to see attacks on critical infrastructure begin in earnest.

Yes, there have already been a few publicized attacks of that variety. And I believe there have been quite a few more that have never been publicized.

But, all signs indicate that attacks by nation-states and anarchists (and even our own governments through agencies like the NSA in the United States) against the types of infrastructure that make modern life what it is will increase and pose a serious threat to individual citizens.

But before we take a look at a range of threats that could challenge citizens in 2015, here is your free copy of the December Self-Reliance Institute Newsletter. It's in PDF format so you can either bookmark it or print it out to save in hard copy format. I hope you enjoy it!

OK, let's get back to the potential threats facing us all in 2015. Today, I'll focus on cyber threats.

But, in coming weeks I'll discuss economic threats as well.

As you know, one of my favorite investigative reporters in the cyber world is Kim Zetter. Zetter is out with a succinct list of potential cyber threats that's worth a gander.

Infrastructure continued page 3

Global Aging and the Stock Market

If you're like me, you view anything and everything from the United States Federal Reserve Bank with a jaundiced eye.

Frankly, I believe "the Fed" is at the heart of many of the fiscal problems here in the United States and around the world.

Still, I'm not one of those who turns my eyes away from data just because of the source.

I was taught at an early age by my parents and by a handful of good teachers to read as much as possible on any topic – but to do so with a critical mind.

In other words, understand who the author is and read very carefully. Watch for words and phrases that don't match the data. But, always look for data or information that can further develop an understanding of the topic or issue being studied.

In fact, I go out of my way to read and listen to those who I am naturally at odds with because it helps me to develop countervailing arguments and to sharpen my perspective on any issue. Over the course of a 15 year career in talk radio, I always brought on guests and callers I disagreed with so that I could dissect

Aging & Markets continued page 5

The American Dream is Gasping for Air

What do you think of when you think of the American Dream?

One common definition of the American Dream is that it consists of a set of ideals in which freedom includes the opportunity for prosperity and success, and an upward social mobility for the family and children, achieved through hard work in a society with few barriers.

To the point, the American Dream is the idea that every American can achieve success and prosperity through hard work, determination, and initiative.

But is the American Dream still alive? Does it still exist? Is hard work, determination and initiative enough to achieve success and prosperity?

"American Entrepreneurship: Dead or Alive?," Jim Clifton

Personally, **I fear the American Dream is gasping for air and may be close to taking its last breath if we don't turn things around fast in this country**.

And I fear that even those of us who have worked hard to earn whatever we've been able to earn may be in danger of losing it if the U.S. stays on the path it is on.

Last week, **I mentioned an article about the impact retiring Baby Boomers might have on the stock market**. And whether or not you have investments in the stock market, you could be impacted because of the effect it could have on the national economy.

Let me point you to the article once again. I'd like you to click on the link, read the article, and share it with your friends and family.

The article you need to check out is, "Federal Reserve: Aging Baby Boomers Will Crush Stock Market by 50%."

Now, let me share something else I saw that has me concerned about the American Dream.

Because for me – and I bet many of you – **the American Dream includes the ability to start our own companies or side businesses. And that part of the American Dream – the part that provides good paying jobs for millions of Americans – has never been at greater risk**.

In a little noticed commentary, "American Entrepreneurship: Dead or Alive?," Jim Clifton, the Chairman and CEO of the famous Gallup polling and analytics company had this to say about the evidence he's seeing when it comes to Americans starting their own businesses.

"***The U.S. now ranks not first, not second, not third, but 12th among developed nations in terms of business startup activity***. *Countries such as Hungary, Denmark, Finland, New Zealand, Sweden, Israel and Italy all have higher startup rates than America does*.

"*We are behind in starting new firms per capita, and this is our single most serious economic problem. Yet it seems like a secret.* ***You never see it mentioned in the media, nor hear from a politician that, for the first time in 35 years, American business deaths now outnumber business births***.

"***The U.S. Census Bureau reports that the total number of new business startups and business closures per year -- the birth and death rates of American companies -- have crossed for the first time since the measurement began***. *I am referring to employer businesses, those with one or more employees, the real engines of economic growth. Four hundred thousand new businesses are being born annually nationwide, while 470,000 per year are dying*.

"*Until 2008, startups outpaced business failures by about 100,000 per year. But in the past six years, that number suddenly turned upside down. There has been an underground earthquake. As you read this, we are at minus 70,000 in terms of business survival…* ***Business startups outpaced business failures by about 100,000 per year until 2008. But in the past six years, that number suddenly reversed, and the net number of U.S. startups versus closures is minus 70,000***.

"*My hunch is that no one talks about the birth and death rates of American business because Wall Street and the White House, no matter which party occupies the latter, are two gigantic institutions of persuasion.* ***The White House needs to keep you in the game because their political party needs your vote. Wall Street needs the stock market to boom, even if that boom is fueled by illusion***. *So both tell us, 'The economy is coming back*.'

The Dream continued page 4

Infrastructure

Continued from page 1

The report is aptly titled, "The Biggest Security Threats We'll Face in 2015," and while I encourage you to read the entire piece, here are a few highlights culminating with the critical infrastructure aspect that I want to emphasize today.

"***Nation-State Attacks:*** *We closed 2014 with new revelations about one of the most significant hacks the NSA and its partnering spy agency, the UK's GCHQ, are known to have committed. That hack involved Belgium's partly state-owned telecom Belgacom...**New revelations about the Regin malware used in the hack, however, show how the attackers also sought to hijack entire telecom networks outside of Belgium so they could take control of base stations and monitor users or intercept communications…These and other efforts the NSA has employed to undermine encryption and install backdoors in systems remain the biggest security threat that computer users face in general***." [emphasis added]

"***Extortion:*** *Controversy still swirls around the Sony hack and the motivation for that breach. But whether the hackers breached Sony's system to extort money or a promise to shelve The Interview, hacker shakedowns are likely to occur again. The Sony hack wasn't the first hacker extortion we've seen. But most of them until now have occurred on a small scale—using so-called ransomware that encrypts a hard drive or locks a user or corporation out of their data or system until money is paid…**This kind of hack requires more skill than low-level ransomware attacks, but could become a bigger problem for prominent targets like Sony that have a lot to lose with a data leak***." [emphasis added]

"***Data-Destruction:*** *The Sony hack announced another kind of threat we haven't seen much in the U.S.: the data destruction threat. This could become more common in 2015. **The attackers behind the breach of Sony Pictures Entertainment didn't just steal data from the company; they also deleted it**…Good data backups can prevent an attack like this from being a major disaster. But **rebuilding systems that are wiped like this is still time-consuming and expensive, and you have to make sure that the backups you restore are thoroughly disinfected so that lingering malware won't re-wipe systems once restored***." [emphasis added]

"***Bank Card Breaches Will Continue:*** *In the last decade there have been numerous high-profile breaches involving the theft of data from millions of bank cards—TJX, Barnes and Noble, Target and Home Depot to name a few. Some of these involved hacking the point-of-sale systems inside a store to steal card data as it traversed a retailer's network; others, like the Barnes and Noble hack, involved skimmers installed on card readers to siphon card data as soon as the card was swiped…**Though card issuers are slowly replacing old bank cards with new EMV cards, retailers have until October 2015 to install new readers that can handle the cards, after which they'll be liable for any fraudulent transactions that occur on cards stolen where the readers are not installed**. Retailers no doubt will drag their feet on adopting the new technology, and card numbers stolen from older DNV cards can still be used for fraudulent online purchases that don't require a PIN or security code. There's also a problem with poor implementation; cards stolen in the recent Home Depot hack show that hackers were able to exploit chip-'n'-PIN processing systems because they were poorly implemented. **With the shift to EMV cards, hackers will simply shift their focus***." [emphasis added]

"***Third-Party Breaches:*** *In recent years we've seen a disturbing trend in so-called third-party hacks, **breaches that focus on one company or service solely for the purpose of obtaining data or access to a more important target**…**A breach of a certificate authority**—such as one involving a Hungarian certificate authority in 2011—**provides hackers with the ability to obtain seemingly legitimate certificates to sign malware and make it look like legitimate software**. Similarly, a breach of Adobe in 2012 gave the attackers access to the company's code-signing server, which they used to sign their malware with a valid Adobe certificate…* ***These kinds of breaches are significant because they undermine the basic trust that users have in the internet's infrastructure."*** [emphasis added]

And here's the one I really want you to pay attention to—

"***Critical Infrastructure:*** *Until now,*

Infrastructure continued page 4

Infrastructure

Continued from Page 3

the most serious breach of critical infrastructure we've seen occurred overseas in Iran when Stuxnet was used to sabotage that country's uranium enrichment program. But ***the days when critical infrastructure in the U.S. will remain untouched are probably drawing to a close****. One sign that hackers are looking at industrial control systems in the U.S. is a breach that occurred in 2012 against Telvent, a maker of smart-grid control software used in portions of the U.S. electrical grid as well as in some oil and gas pipeline and water systems. The hackers gained access to project files for the company's SCADA system. Vendors like Telvent use project files to program the industrial control systems of customers and have full rights to modify anything in a customer's system through these files. Infected project files were one of the methods that Stuxnet used to gain access to Iran's uranium-enrichment systems.* ***Hackers can use project files to infect customers or use the access that companies like Telvent have to customer networks to study the customer's operations for vulnerabilities and gain remote access to their control networks. Just like hackers used third-party systems to gain access to Target, it's only a matter of time before they use companies like Telvent to gain access to critical industrial controls—if they haven't already****." [emphasis added]

OK. There's a broad over view of cyber threats. I encourage you to read the entire piece, but those highlights give you a flavor of what we may be facing.

And **it's the Critical Infrastructure threat that should concern us the most**. After all, replacing credit cards after a hack like Target is an annoyance – a big annoyance. And identity theft is a serious crime that I work to combat as a security professional every day.

But, if hackers can take over portions of a nation's electrical grid, or a nuclear power plant, or the interconnectivity of the financial network, or – well, you get the point.

The reality is a successful attack against Critical Infrastructure could bring the United States – or any other country – to a standstill for enough time to create panic, chaos and, potentially, anarchy.

So I pose to you the question that I repeat so often: **Are you and your loved ones self-reliant enough to live on your own – without the assistance of the government or critical infrastructure like electricity and water – for an extended period of time?**

I hope so. I really hope so. Because as I've documented many times before, there is a significant chance that in your lifetime you will have to do so.

OK. Enough of my thoughts. What do you think?

Email me at Rob@SelfRely.com and let me know if you believe there are significant threats to our nation's infrastructure.

I look forward to your comments.

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective

PS – For a recent example of what can happen when hackers take control of an industrial facility, check out "Cyber Attack Causes Physical Damage at German Iron Plant."

The Dream

Continued from page 2

"***Let's get one thing clear: This economy is never truly coming back unless we reverse the birth and death trends of American businesses***. …

"***I don't want to sound like a doomsayer, but when small and medium-sized businesses are dying faster than they're being born, so is free enterprise. And when free enterprise dies, America dies with it***."

OK. It pains me to share that brutally honest, fact-based assessment from the top man at Gallup. (If you want to read the entire commentary, click Here.)

But if we are to save the American Dream for future generations of Americans – and ourselves! – we must be honest with one another and we must realize that so much of what we hear from the White House, Congress and Wall Street is nothing more than a pack of lies.

And, as the evidence suggests, they are lying while the America we love is dying!

The Dream continued page 6

Aging & Markets

Continued from Page 1

their arguments. (Besides, it was more fun that way!)

Bottom line: I believe those who just read or listen to those who they always agree with develop weak minds and show little ability to understand a topic more than an inch deep. They live in an echo chamber that deafens them to important information.

As members of the Self-Reliance Institute, I suspect you have and seek the ability to read and think critically as well.

So, in that vein, I want to share an Economic Letter that was released by the Federal Reserve Bank of San Francisco just before Christmas. The letter is headlined, "Global Aging: More Headwinds for U.S. Stocks?"

Here's the conclusory paragraph that the authors put up front:

"The retirement of the baby boomers is expected to severely cut U.S. stock values in the near future. Since population aging is widespread across the world's largest countries, this raises the question of whether global aging could adversely affect the U.S. equity market even further. However, the strong relationship between demographics and equity values in this country do not hold true in other industrial countries. This suggests that global aging is unlikely to create additional headwinds for U.S. equities."

OK. If we just take those four sentences at face value, it would be easy to not read any further and conclude that the San Francisco Fed wants us to believe that while the aging of the U.S. population could impact U.S. stock values "in the near future," "global aging" will not add any additional downward pressure on those stocks.

Additionally, if you do read the letter further, you'll find the usual wishy-washy statements that economists almost always include in everything they write so that they can claim later they weren't wrong no matter what happens.

"Let's read the letter with a critical mind. . ."

Therefore, it'd be easy to look at this letter and ignore it because: A) It's from the Fed and I rarely trust the Fed, and B) It's filled with a lot of language designed to protect the authors' credibility no matter what the future brings.

So if you ignore the letter, I'll understand why.

I'll also think you're making a big mistake.

Here's why.

Let's read the letter with a critical mind and see if it contains any important and indisputable facts that we can take away after all the other verbiage and charts and economists' mumbo-jumbo.

If we read the letter that way, I believe there is a key fact and conclusion that could impact our thinking when it comes to investments for the foreseeable future.

That fact and conclusion is contained in this statement from the letter:

"[P]rojected declines in stock values based on these data have become even more severe. Our current estimate suggests that the P/E ratio of the U.S. equity market could be halved by 2025 relative to its 2013 level."

In plain English, that means ignore all the other information in this letter about "Global Aging" and the stock market because if you read closely you'll find that information is speculative – it's a guess at best.

The one solid fact in this report is that when it comes to the U.S. Stock Market, the aging of the population here in the United States could cut the price of stocks in half over the next 10 years.

So the question we must ask ourselves is:

Why would anyone invest in a stock market that could drop by 50% over just the next decade?

I suppose we'd all answer that question differently. But I know how I look at the one projection in the Economic Letter that is based in fact – not speculation.

I look at that fact and it reinforces my instinct and current economic view in a way that I'll be looking for Alternative Investments from the U.S. Stock Market.

OK. That's a lot to chew on. But I'd love to hear what you think.

Write me at Rob@SelfRely.com and let me know if you believe the U.S. Stock Market is the safest place to invest over the next 10 years or if we all should be looking for Alternative Investments.

If so, what investments do you believe are better/safer than the stock market?

As a relevant aside, do you believe the stock market is rigged?

I look forward to your emails!

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective

Phishing

Continued from page 1

ulating people so they give up confidential information.

Stated more simply, social engineering is the scam.

It's the con (confidence game) of the con man.

Now, to be sure, the poster I located is directed at employees of companies that are constantly bombarded by phishing emails.

Still, almost all the Red Flag warnings on the poster are applicable for everyone.

Please review the poster (it's in pdf format), Social Engineering Red Flags, created by the good people at KnowBe4.

You can print it, download it (pdf format), or bookmark it as a readily available document you can review from time to time as a way to stay on guard against phishing emails.

OK. As I said, some of it is in language referencing employment circumstances, but almost all of it applies to any phishing email.

And, the poster breaks the various parts of an email out separately so you know the warning signs of a scam phishing email that may show up in the following categories:

From:
To:
Subject:
Date:
Hyperlinks:
Content:
Attachments:

Alright. Please review the poster. It won't take more than a minute or two and it's a great refresher about what to watch out for when opening emails. You'll probably even learn about a few red flags you didn't know about.

And you can always email me at Rob@SelfRely.com with any questions about a possible phishing email scam. I'm always here to help.

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective and Certified Identity Theft Risk Management Specialist

The Dream

Continued from page 4

OK, it's your turn.

Tell me what you think about the American Dream.

Is it alive and well?

Or, is it being killed by the liars in Washington DC and on Wall Street?

Email me at Rob@SelfRely.com and share your thoughts.

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective

Self-Reliance Institute Newsletter

Privacy:
HERE'S THE BOTTOM LINE: WE WILL NOT EVER GIVE, SELL, OR RENT YOUR INFORMATION TO ANYONE – EVER.

Questions or comments?

Please email me at Chris@SelfRely.com or call me at my Freedom Writer's Publishing office at 970-367-7624.

http://www.SelfRely.com

Protecting your privacy. Giving you more security.