Self-Reliance Institute Newsletter

January 2015 Volume 3, Issue 01

Sharpen Your Ability to Spot Phish

The other day, a friend asked me why so many people become victimized by malware (malicious software) that damages and steals information from personal computers and other electronic devices that are connected to the Internet.

Without even hesitating, I said, "Because they get tricked into clicking on links in emails and websites that plant the malware on their device. At that point, it's almost always too late to stop the bad consequences."

My friend then asked, "What's the best way to not "get tricked?"

Good question.

The easy answer is, "Don't ever click on a link in an email that you're not 100% certain is from a legitimate source. Otherwise, you may be the victim of a phishing email (an email that tricks you into providing personal and financial information used for identity theft and other forms of fraud) or you may unknowingly download malware that harms your computer."

Phishing continued page 4

IN THIS ISSUE

A Gross Economic Warning

If you only focus on the stock market and the mainstream media reports about the successes of those getting rich on Wall Street - because they have privileged access to what is undoubtedly a rigged game at this point - you'd think all is right in America.
But is that the reality that most of us are experiencing?

The other morning, I got a haircut at my regular barber shop from a barber I didn't recognize. As we chatted, the barber mentioned she was new to town. So I asked what had brought her to our community.

In short, after several decades of owning her own hairstyling shop in another state, her business had failed. What had once been a thriving enterprise, had slowly succumbed to a long stagnant local economy and she could no longer afford to keep the doors open.

To make matters worse, when she sold her house so she could move to find work and to be closer to her daughter, her house only sold for what she'd paid for it many years earlier.

From there, we talked about how difficult it is to run your own business and how income and wages for many working Americans haven't improved since the late 1970's.

Economy continued page 3

The Package Delivery Scam

Rob here.
I know this is a very busy weekend for a lot of you as you finish up holiday shopping and get ready to travel or welcome guests. In fact, many of you may already be on the road or already have guests in the house.

So, I'll be very brief while warning you about a scam I want to be sure you avoid.

The most effective scam this month is **the Package Delivery Scam**.

It's effective for the precise reason I'm being brief – **because everyone is busy and when we're busy we're far more likely to click on a link in an email that we'd normally realize is a phishing email scam**.

As you know, phishing email are email that request confidential information under false pretenses in order to fraudulently obtain credit card numbers, passwords, or other personal data.

Here's how the current and most prevalent Package Delivery Scam works (but remember, there are many variations of this scam).

You receive a "delivery failure notification" email that looks like it's from

Pkg Scam continued page 7

ObamaCare and Health Record Privacy

The other day, I sent the following alert (between the two sets of five dashes a bit further down the page) to our Privacy and Security list. While some of you may have seen it there, I want to share it again for a very specific reason.

The reason is because I got flooded – deluged – with email comments about ObamaCare and the loss of privacy when it comes to our health records. Overwhelmingly, the folks who wrote me did so to let me know how upset they are with the federal government's plan to share our records with so many government agencies.

In fact, out of all the email I received, only one individual felt the need to defend the government and to tell me I am wrong because the data that will be shared will not be able to be tracked back to specific citizens.

Friends, I do make mistakes from time to time. But this is not one of those times. I work very hard to be sure that the information I send you is accurate and that the conclusions I draw are based on facts – not conjecture or speculation.

So today I want to empower you with even more information about the reality that **your health records are going to be shared between dozens of federal agencies and if the government decides to track a record back to you it can**.

So first read the original alert I authored (between the two sets of five dashes) and then I'll add some additional information after the second set of dashes.

---

35 Agencies Will Get Your Health Records

As many of us feared and predicted about ObamaCare, it is true that your health records will be shared near and far when it comes to the federal government.

And of course the feds don't want you to notice the latest news, so they've released it during the holiday season when folks have less time to pay attention to the news as they're shopping for gifts and finishing end of year projects at work.

But you need to know this, so here it is.

The report you need to read, "**Feds Plan for 35 Agencies to Help Collect, Share, Use Electronic Health Info,**" is from The Weekly Standard.

While I encourage you to read the report, here are the most important details.

"*This week, the Department of Health and Human Services (HHS) announced the release of the Federal Health IT Strategic Plan 2015-2020, which details the efforts of some* ***35 departments and agencies of the federal government and their roles in the plan to 'advance the collection, sharing, and use of electronic health information to improve health care, individual and community health, and research***.'"

What departments and agencies?

Check out this list:

- Administration for Children & Families
- Administration for Community Living
- Agency for Healthcare Research and Quality
- Centers for Disease Control and Prevention
- Centers for Medicare & Medicaid Services
- Department of Agriculture
- Department of Defense
- Department of Education
- Department of Justice and Bureau of Prisons
- Department of Labor
- Department of Veteran Affairs
- Federal Communications Commission
- Federal Health Architecture
- Federal Trade Commission
- Food and Drug Administration
- Health Resources and Services Administration
- HHS Assistant Secretary for Financial Resources
- HHS (Health and Human Services) Assistant Secretary for Health
- HHS Assistant Secretary for Legislation
- HHS Assistant Secretary for Planning and Evaluation
- HHS Assistant Secretary for Preparedness and Response
- HHS Office of the National Coordinator for Health Information Technology
- HHS Office for Civil Rights
- HHS Office of the Chief Information Officer
- HHS Office of the Chief Technology Officer

ObamaCare continued page 5

Economy

Continued from page 1

Which is, of course, demonstrably true.

I left the barber shop contemplating this sad reality and thinking about this lovely woman who is at an age when she should be preparing for retirement but will never be able to retire unless she hits the lottery.

Then I walked in my office and saw this headline on Zero Hedge.

"It's All Coming to an End, Bill Gross Warns."

Talk about a not-so-cheery start to the day!

But as much as I wanted to ignore the report and put on some uplifting music as I sat down to work, I had to read what Bill Gross – a well-known and well-respected bond investor – had to say.

After all, Gross is not an alarmist. He's not a fringe figure. He's a mainstream investor who has a proven track record of looking to the horizon and making ahead of the curve decisions based on sound analysis of what present monetary and fiscal policy may mean down the road.

And while I invite you to read all of what Gross had to say – **you can do so by clicking here** – I'll boil it down for you as his writing style is a bit obtuse.

Gross believes future generations – our children and grandchildren – will look back at the monetary and fiscal policymakers of today and ask, "How could they?"

In other words, **"How could they have been so wrong?" "How could they have done so much damage?"**

Specifically, after analyzing how policymakers failed to solve our ongoing debt crisis by creating more debt – something most all of us with common sense knew wouldn't work – Gross states:

"It is difficult to envision a return to normalcy within my lifetime…I suspect future generations will be asking current policymakers…

"How could they? How could policymakers have allowed so much debt to be created in the first place, and then failed to regulate their own system accordingly? How could they have thought that money printing and debt creation could create wealth instead of just more and more debt? How could fiscal authorities have stood by and attempted to balance budgets as opposed to borrowing cheaply and investing the proceeds in infrastructure and innovation? It has been a nursery rhyme experience for sure, but more than likely without a fairytale ending."

Excellent questions!

However, unlike Gross, I don't think these are questions that will only be asked by future generations.

I think these are questions that can be asked today.

In fact, I suspect this confirms what many of you have known for quite some time – something I used to discuss frequently on my former radio show – the power brokers of Wall Street and Washington, DC are working together to enrich themselves and their contributors while the rest of us are left to fend for ourselves in an unfavorable economy.

Those power brokers – those insiders – know that a day of economic reckoning is coming. And their plan is to enrich themselves as much as possible before that day arrives.

Think about it. That apparent reality answers all of Bill Gross' questions.

They've intentionally designed the money printing and debt creation as a means of immediate wealth creation for the few at the expense of the many.

They know it won't last because it can't last.

But that doesn't matter to them as they're grabbing all they can before the economic house of cards they've created implodes.

So what are we to do? What can normal folks like you and me do?

We have to think outside the box.

We have to look at alternative ways of creating wealth.

Most important, we have to realize that the day of economic reckoning for the United States is coming because of the greed of those currently in power.

So we must prepare for that day.

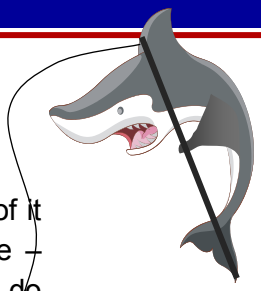
As we turn the calendar page from 2014 to 2015, I will begin to discuss those preparations and alternative wealth creation possibilities on a more frequent basis.

But today, I'd like to hear from you.

Economy continued page 4

Phishing

Continued from Page 1



But the reality is that it's getting harder to spot phishing emails and/or emails that trick you into clicking on a link or going to a website that downloads malware onto your device.

The criminals are getting more sophisticated with the fraudulent emails they send and websites they create to commit their crimes.

To demonstrate that reality, I'm going to suggest that you check out two articles I bookmarked earlier this month and take a test to see if you can identify fraudulent emails – phish.

The first article, "Can you spot the phishing scams and stay safe online? " provides a few Do's and Don'ts when it comes to spotting and dealing with phish and other malicious emails.

But, equally as important, that article mentions an Interactive Phishing Quiz that Intel Security and CBS News created so that folks can test their ability to differentiate between a phishing scam vs. a legitimate email.

That quiz can be found at the bottom of the article, "**Phishing quiz: Can you spot a scam when you see one? Don't be so sure.**"

And I have a suggestion to make the test as clean as possible. First, before you read any of the other material in those articles, take the interactive quiz at the bottom of the page linked in the paragraph before this and see how you score.

I only scored 80%. That score puts me ahead of most security professionals – but I still was tricked a couple of times.

So for the fun of it – the challenge – see how you do and then read the suggestions in the articles.

But, most important, I want you to develop a mindset where you are suspicious of every email you receive until you examine it and determine that it's safe.

Whenever in doubt – any doubt – don't click on a link in a suspicious or unexpected email. If it purports to be from a website that you do business with, ignore the provided links and go directly to that website from a link you've previously bookmarked. If the email is genuine, all the data and links you need will be at the website you went to independent from the email.

Yes, I know. It's sad that in this day and age we can't even trust email. But that's the reality we live with today.

As always, please email me your questions and comments – Rob@SelfRely.com

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective

Economy

Continued from page 3

I'd like to know whether you agree with Bill Gross.

Do you believe that the current monetary policy of money printing and debt creation is wrong?

Do you have alternative wealth creation ideas or strategies that have worked for you?

Do you believe the folks on Wall Street and in Washington, DC are working honestly to improve the economy for everyone or are they just looking out for themselves?

Please email me at Rob@SelfRely.com with your thoughts and together we'll move forward into 2015 with a goal of improving the lives of good people like the barber who shared her story with me the other day.

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Investigator

ObamaCare

Continued from Page 2

- HHS Office of the General Counsel
- HHS Office of Minority Health
- HHS Office of the Secretary
- Indian Health Services
- National Aeronautics and Space Administration
- National Institutes of Health
- National Institute of Standards and Technology
- National Science Foundation
- Networking and Information Technology Research and Development
- Office of Personnel Management
- Social Security Administration
- Substance Abuse and Mental Health Services Administration

By the way, The Weekly Standard counts 35 departments and agencies. I count 37 on the list.

But hey, any way you look at it, that's an awful lots of federal agencies and federal employees who will have access to your health records.

I suspect this confirms what many of you knew would be one of the realities of ObamaCare, but there it is in black and white.

And, I suspect this is just the beginning.

As an information security expert, I can tell you that there is no way – NO WAY – that the feds will be able to keep your health records secure with that many federal agencies having some type of access.

The only questions are:

Should ObamaCare be repealed?

Can ObamaCare be repealed?

Let me know your thoughts by emailing me at Rob@SelfRely.com Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective

OK. That was the original alert I sent to tens of thousands of good citizens like you.

And, as I mentioned, I received a huge amount of email in response from folks who are upset about the way the federal government is sharing our health records.

Still, I received an email from a gentleman who felt I was being "alarmist" because he's been part of a university study for an extended period of time and they anonymize his records by labeling them with a code instead of his name. Therefore, he (and, in truth, many other

unwitting citizens) is comfortable with his data being shared as long as it doesn't go beyond identifying him with demographic data like age, sex, race, city and state.

In short, he clearly believes his health and medical record can be used for scientific study and his privacy preserved because he has been "deidentified."

But, as we should all know as free-thinking adults, there is what can be done and what is actually being done.

So yes, in theory, a law could be passed and a system could be designed that would prevent the government from identifying you from the health records they are going to collect under the authority of Obamacare.

Those records could be anonymized and deidentified.

But is that the current state of the law? Will it be impossible for a federal agency or employee or agent to know who a specific health record belongs to?

I think not.

I believe the government will remain able – both legally and procedurally – to identify the individual citizen who is associated with a so-called anonymized or deidentified health record.

But don't base your assessment on my thoughts and beliefs.

Instead, let's look at an article that specifically addresses the question and the underlying work of those who fight the government over privacy issues every day.

The article, "**38 Government Agencies to Collect, Share American's Electronic Health Records**," was published this week by Network World. While the article says much of what I said in my original alert about this topic, at the end it adds a reference to a report co-written by Jim Dempsey from the Center for Democracy and Technology – a private organization that fights the government over privacy issues.

[As an aside, I know Dempsey personally and have testified about privacy issues alongside him before Congress on more than one occasion. Jim is one of the strongest advocates for individual freedom and

ObamaCare continued page 6

ObamaCare

Continued from Page 5

privacy in the U.S. and has been fighting the good fight for many, many years.]

That report, "**Privacy as an Enabler, Not an Impediment: Building Trust into Health Information Exchange**," examines many public and private policy and legal issues that impede our ability as citizens to keep our health and medical records private.

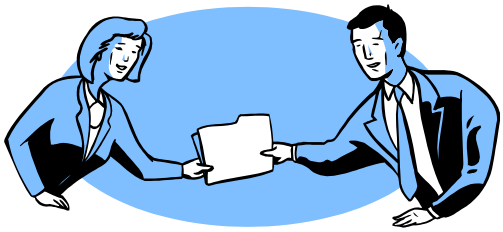
Among those issues is a key section that is relevant to the issue of so-called anonymized and deidentified health records now that so many government agencies and employees will have access to our health records.

The section is titled, appropriately enough, "Deidentification," and states:

"***HIPAA's (the federal healthcare privacy law) protections do not extend to "deidentified" health information***. *Thus, covered entities may provide deidentified data to third parties for uses such as research and business intelligence without regard to HIPAA. In turn, these entities may use these data as they wish, subject only to the terms of any applicable contractual provisions (or state laws that might apply).* ***If a third party then reidentifies these data—for example, by using information in its possession or available in a public database—the reidentified personal health information would not be subject to HIPAA***. *It could be used for any purpose unless the entity holding the reidentified data was a covered entity.*" [emphasis added]

And then this:

"***A number of researchers have documented how easy it is to reidentify deidentified data***. *The U.S. Department of Health and Human Services (HHS) should revisit the current deidentification standard in the Privacy Rule (in particular, the so-called safe harbor that deems data to be deidentified if*



they are stripped of particular data points), to ensure that it continues to present minimal risk of reidentification. At the same time, HHS and Congress should work together to ensure that recipients of these anonymized data are accountable if the information is reidentified." [emphasis added]

Bottom line: **While the federal government may state that our health records will be "deidentified" from us as individuals, it is a well-known and documented fact that it is "easy" to "reidentify" "deidentified data."**

In short, the federal government will have the ability to track medical data back to a specific individual and it appears that currently it would not be illegal under HIPPA if that happens.

OK, I apologize for the length of this week's advisory. But, I always want you to have the information you need to combat those who spread false information.

In this case, anyone who says the more than three dozen federal agencies that will have access to American's health records will not be able to identify individual citizens from those records because of anonymizing and deidentification procedures is incorrect.

It has been proven that deidentified records can easily be reidentified.

Feel free to share your comments and thoughts with me at **Rob@SelfRely.com**

Be safe, secure and free!

Rob Douglas – Former Washington DC Private Detective

PS – While I focused today on the reality that deidentified records can easily be reidentified, if you review the rest of "**Privacy as an Enabler, Not an Impediment: Building Trust into Health Information Exchange**," you'll see that there are many other legitimate and documentable concerns when it comes to the privacy and security of our health records now that they are being digitalized and shared.

Pkg Scam

Continued from Page 1

the U.S. Postal Service (or FedEx or UPS or any other delivery company). The email says you missed a delivery. But, it says, if you print the attached form and take it to your local post office (or other delivery company), you can pick up your package and avoid penalties. Often, the email includes a link for more details.

Of course, the email is a scam and there is no package. But, if you open or download the attachment or click on any link in the email, you're likely to end up with a virus or malware on your device.

OK. I know this might be fairly basic for most of us. But, **you be amazed how many times even the most careful and scam-aware computer users click on the link in an email before pausing to think about whether the email might be a malware-laden phish.**

I can tell you I've received many calls over the years from clients and friends that begin with, "Rob, I know better, but I clicked on the link in an email and…"

So here's my motto: **Think before you link**!!

OK – you get the picture. I promised I'd be brief, but I just want to be sure that you **don't fall for the Package Delivery Scam this week – when more packages will be delivered than most any other week of the year!**

If you have any thoughts, comments or questions – email me at Rob@SelfRely.com and be sure to share this advisory with your family and friends.
Otherwise, have a wonderful holiday week and…

Be safe, secure and free!!!

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

PS – If you want a quick refresher on malware, the FTC has a fairly good page on the topic located **HERE**.

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