COMPUTER CORNER

I've Been Hacked!

By Mike@Blackledge.com

"Excuse me, ma'am, we've received a report that your computer is running slow – is that correct?" The voice on the phone is authoritative, yet with a foreign accent. And thus begins an adventure into computer insecurity, an adventure you don't want – or need.

We genealogists depend on our computers for maintaining our data and access to the Internet for conducting our research. And our computers seem to run slower each year, primarily as we add more programs, browser extensions, and start-up 'features.'[1] Thus genealogists, like most computer users, may well be tempted by this unsolicited phone call to "solve our problem."

My wife received three of these calls, spaced by a few days. On the fourth, I answered and got "Alex" with a very heavy (Indian? Asian?) accent. He said he was from HelpTech247, and that when I browsed the Internet, some unwanted files are getting downloaded to my computer. HelpTech247 could put me in a "SafeZone". When I asked him where he was calling from, he repeated "HelpTech247." When I said, "But what country are you in right now?" – and the call ended. (On one of my wife's calls, the female caller said she was calling from The Virgin Islands.) I Googled for HelpTech 247 and found my experience is similar to this report posted on scambook.com in Sept 2013, although Alex never mentioned Microsoft or a virus:

> *I received a call from a man (Indian or Asian accent) claiming to be from helptech247. He said they were representing Microsoft & had 'detected' a virus on my computer. When I started asking questions about how they got my name, address & phone number he got upset & started telling me if I didn't use his help now, I would be responsible for my computer ceasing to operate.*

You don't need to go any farther with these people. Please *don't* go any farther with these people – they are much better at what they are going to do than you are to control it. What they want to do is to have you initiate a remote access and file sharing tool that is on all Windows operating systems. In malware terms, programs that access your computer *without* your permission are known as backdoors, password

[1] A computer training colleague at Sandia would comment, "The faster computers get, the more impatient we are."

stealers, and data theft Trojans. Here you are actually giving some stranger permission to run this remote access program on your computer. When you do so, you are connecting to the Internet and providing access to your computer to a complete stranger, one who is very good at doing what he is going to do. At the very least, he is going to charge you hundreds of dollars for this "service." At the worst, he is going to gain access to your personal information, easily to include your contact list.

Your Caller ID may read **Private Caller** (with no phone number) or **Out Of Area**, or Private and perhaps a number like 901-807-7856. That example happens to be a Memphis, TN number, and if you Google for it, a phone number complaint collection site such as WhoCalledMe.com or 800Notes.com will present a plethora of comments, e.g.,

> *"Some Indian guy - calling because he detected my PC was running slow and was following up on a trouble ticket that I called in. Told him I didn't own a PC, he said - well, I am showing that there is one in your house and he told me to give him all my data so he could look into it." "Called to indicate my computer was running slow and wanted to fix it." "Gentleman with an Indian accent called saying he was getting reports of my computer running slow. I asked him which one and he said my home computer (there are three desktops and five laptops in our house)."*

The phone number identified is immaterial. The actual caller may well be in another country and has access to this 'legitimate' USA number as a transfer point. You can't call the number back. If you ask too many questions, they will hang up. A colleague of mine, a lawyer in Albuquerque, replied to a similar unsolicited inquiry, "Yes, it is slow!" The next step? They take over your computer by remote, and sure enough, identify some 'problems' – and perhaps they even make it faster. Then they present a bill for several hundred dollars. Whose fault is this? My lawyer friend used what I call the "Open Kimono Approach" – you open your computer to some complete stranger with skills in electronic hunting and gathering, and in effect say, "Here's all my computer information, passwords, financial and private information – see anything you like?"

His friends found out about all this weeks or months later, when we received an email "from" our lawyer friend, with that message about being stuck in London or Buenos Aires or wherever, losing his passport and wallet, and needing us to wire him some money, please. These money scams are getting more sophisticated – at one time, say in 2008, they contained obvious spelling and grammar errors. Now they look pretty clean. And they are addressed to you, from your friend.

The point is, once you open your computer to remote access, everything is 'fair game.' The scammer can easily collect your contact list of email addresses and immediately sell it to other awaiting scammers for their uses. Of course, serious identity theft could also result.

Why AOL? As a point of interest, 15% of AGS members have AOL email addresses, and another 11% have either Yahoo or Hotmail accounts. Those are certainly legitimate

services[2], but as anecdotal evidence, it appears that the majority of the hacked email spams are from AOL customers. Why would this be? Excuse me AOL people, but most AOL users tend to be older and many are less sophisticated computer users. Thus their passwords might be some of the most common, such as 1234567, 1111111, Password, etc.[3] A column appeared in the *Daily Intelligencer* in Feb 2013 under the title *Why Rich, Famous, and Old People Need to Ditch Their AOL E-mails*. The author Joe Coscarelli makes the following points:

> *For reasons we cannot comprehend, some of the most important people in the world (who also happen to be old) have not yet migrated to Gmail[4], the generally agreed upon leader in e-mail technology, opting to stay with an out-of-date service (see also: Yahoo, Hotmail, Earthlink) and leave themselves vulnerable to security breaches that don't even require any expertise. Back in 2011, Ben Smith explored the "generation of the political and media elite" who keep AOL accounts: "virtually the only people I email at AOL accounts are bigshots — people who were already so important by the time the various new fads (and technical advantages) arrived that they couldn't be bothered to switch, and had nothing to prove to anyone." On his list at the time: David Axelrod, Matt Drudge, David Brooks, and more.*
> *Our digital lives are simply too easy to crack. Imagine that I want to get into your email. Let's say you're on AOL. All I need to do is go to the website and supply your name plus maybe the city you were born in, info that's easy to find in the age of Google. With that, AOL gives me a password reset, and I can log in as you.*

What do I do if I've been hacked? You'll know pretty quickly once it happens – you'll find some bounce-back messages in your in-box from some of your old contacts who no longer use the address you list for them. And friends will start calling you and emailing you. Many friends. So here's what you do: 1. Change your password, and 2. Apologize to your friends for asking for money.

Two-step Verification: One of my many reasons that Gmail (and sponsor Google) is more secure is that they employ 2-step verification. The theory behind this system is that it is highly unlikely that your computer and your phone would both be compromised at the same time. (If they are, you need to close your old accounts and start over!). When you login to your Gmail account at a physical location not recognized in your profile, Google asks to send a code to you on your (registered) cell phone.

---

[2] I have a friend who continues to have AOL charge his credit card each month. AOL has been a free service since 2006, but they are delighted that people continue to pay them anyway.

[3] When some 400,000 passwords were hacked in the famous Yahoo! Voices hack of July 2012, some analysis showed that 38% of them were 123456 and another 18% were Password.

[4] Despite the persuasive article *"Gmail for Genealogists"* of Feb 2012 that appeared in this column, only 9% of AGS members list a gmail.com email address. Gmail encourages **two step verification** to prevent unauthorized users.

You can override this request; if you do, Google will send you a report (later) listing the place and dates and times when your Gmail account was used. If you enter the code, you are good to go at your new location.

How did they get my password? This is the next question you need to answer. You need to know this so you can prevent them from getting your new password! Here are some possibilities from Rich Pasco:

1. **They guessed it** or discovered it by trial and error. Bad passwords include your name, your birthday, a word from the dictionary, etc.

2. **They obtained it from your service provider** by clicking "lost password" and answering your security questions with information they know about you (genealogy info such as your mother's maiden name, childhood pet, etc.) As we've seen, AOL folks can be quite helpful here!

3. **You gave it to them,** by typing it into their web site. The strongest password in the world is no good if you give it away for the asking! Maybe the web site was a phony one mimicking the login screen for your e-mail service. Or maybe it promised some freebie (e.g. cup of coffee) if you just enter your e-mail address and password. A social networking site may ask for your e-mail password to invite your friends to join their network. Or you may get a phony e-mail, ostensibly from your service provider, asking you to click on a link to a form and enter your information to "confirm" your account.

4. **You used the same password on another site.** Many web services require you to sign up with a username and password. Do *not* choose the same password as for your e-mail account! Doing so would give the operator of that site access to your e-mail account, to read your mail and to send out mail in your name.

5. **A "spyware" program in your computer** (or a public computer you used) saw it. Spyware is malicious software which runs stealthily in the background, virtually looking over your shoulder and sending what you type back to its headquarters. One form of spyware, *key logging* software, quietly records every keystroke you make. Many virus scanners do not detect spyware, so you should periodically scan your computer with a specific spyware scanner. One I recommend for Windows users is Spybot Search and Destroy; another is Malwarebytes Anti-Malware Free.

What's a better password? We could spend half a column on this, and perhaps we will someday.[5] The references provide help, but here is a short answer: To thwart computer hacking, any 12 characters are better than any 8 characters. But how to remember? Let's say that you have a favorite password (doesn't everyone?), e.g., the name of your dog and when she died: Dorcas11. Then you can easily remember and use a different password on every site by putting some security padding before (and after?) your standard password. For

[5] Send an email to mike@blackledge.com with your suggestions for future column discussions.

example, the password when you log onto Facebook could be FaceDorcas11, and the password when you log onto Costco.com could be CostDorcas11. Even better would be to add a bang (!) at the end.

Summary: This article hopes to thwart computer scams. Often the underlying concern for people responding to these scams today is that their computer is slow. Viruses and spyware could be the culprit, but the primary reason for a computer slowing down is the additional software we have loaded onto it, whether desired or not.

Believe it or not, there are some unscrupulous people in this world who are willing to take advantage of you based on your fears. Some will go to great effort to charge you for services you do not need; a few enjoy just being malicious. Most of them are not genealogists and would love to run a remote access program on your computer, and gain access to your credit card or other identity info. Some closing thoughts:

1. If you grant remote access to your computer, you are indicating an extreme amount of trust. Ask yourself: if this person came to my door, would I invite them in and give them my computer password? Trust should be earned over time, not during a cold phone call.
2. You are under no obligation to answer or respond to phone calls, emails, or even knocks on your front door. I learned this from the late Walter White.
3. We all want access to the resources on the Internet. Keep in mind: access to the Internet infers that the Internet has access to you! (Perhaps this is why some of us prefer to deal with dead people, e.g., FindAGrave.com)
4. Consider ways to check out a business before you entrust them with your credit card. If you can't call a company back, something is wrong. If you must decide on a service or a purchase "right now," then "No" is the best answer. Take some time and check them out – Angie's List may well be worth the cost!

References: There is a plethora of information on these topics. You can find these articles on-line:

- 2 million Facebook, Gmail and Twitter passwords stolen in massive hack byJose Pagliery,*CNN Money,*, December 4, 2013
- The worst passwords you could ever choose exposed by Yahoo Voices hack by Graham Cluley, *Sophos Naked Security,* July 13, 2012
- How I'd hack your passwords byJohn Pozadzides, MSN Money, February 4, 2011
- Choosing a smart password from Google
- About 2-step verification from Google