All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

I've been Hacked! What do I do?

One of my readers recently asked me a question that I get every once in a while. It's not a corporate high consequence national security life and death question. It's a simple one. A regular human being, without a whole lot of resources, thinks (or knows) they have been (are still being) hacked. What do they do?

No real resources

Most people do not have a lot of resources to spend on their personal or family cyber security program. And almost nobody out there will or reasonably can spend hours and hours helping them for free. The anti-virus companies and similar entities, including many ISPs provide some sort of program to help their customers, but once someone has broken in, the cost skyrockets. You can go to your local PC repair shop and let them give it a go, but odds are the bad folks have access to many of your accounts because they have passwords and user IDs to many of them after they have sniffed your keyboard and network connections for a while.

Some things you can do for relatively little

A strategy I have advised many folks on for many years in such situations, and one I use myself for "small" issues is basically this:

- Assume everything you have has been hacked.
- Start with something reasonably secure pristine from the factory.
- Get the most important resources under control.
- Over time re-engage with the other things of your digital life.

Note that the specifics change over time, and I recall having written an article like this 20 years or so ago, but things have obviously changed since then.

A practical example for today

Here's the outline of a step-by-step process to get from unsafe to more safe that works reasonably well today for relatively little money. Note that things change – and this is not perfect (nothing is). But for the average user in a relatively prosperous world, it is a good path forward that you can do on your own.

Assume the worst

STOP using your existing digital resources.

- Disconnect your current computer(s) from networks while you take the next steps.
- I favor turning them off, but likely you will need them on in order to get access to your passwords and similar things.
- **Get a (reasonably) secure anchor point: GET** a cheap new Chromebook ($250) and (optionally for the last step) a 4 Tbyte USB hard drive ($100).

- Why a cheap Chromebook? Because they are cheap and relatively secure and capable of doing most of the critical stuff most people need to do with their computers. Even if it is your phone that has been hacked, you will want to do this.
- Why a 4 Tbyte USB hard drive? They are cheap for the quantity of storage and have enough storage for most of what regular people will need for some time to come. They can also be easily connected to lots of systems.

Get control over the critical stuff:

RESET the passwords on all of your most critical accounts.

- The first thing you should do with your chromebook is get a **NEW FREE** gmail account. **DO NOT USE YOUR OLD ANYTHING AT ALL AT THIS POINT.**
  - Why a new free account? Because it has not yet been hacked, and from your new chromebook, which has no other accounts, it will help assure that your chromebook has also not yet been hacked.
  - Why not use your existing anything? Because we don't want to infect the Chromebook with anything from any outside source and we don't want to be watched through other digital systems as we do these first operations.
    - **DO NOT** use any of your existing peripheral devices yet.
    - **DO NOT** use any existing accounts on any systems yet.
    - **DO NOT** connect to any of your online resources yet.
    - **DO NOT** use your computer in front of anything with a digital camera.
    - You might reasonably use your existing wireless connection because almost all of the things we are doing are encrypted end to end. It's up to you if you prefer the local library or coffee shop and its free Internet access. However, a public place means others might be able to view your screen and keyboard – and get access to your accounts.
- The second step, after getting an initial cloud-based account you can work from, is to gain access to your critical online accounts.
  - What is a critical account?
    - That's up to you. I usually suggest starting with financial system accounts (your bank, your broker, your bookkeeping systems, etc.) because they can do you the most financial harm, and the bad folks the most financial gain.
    - You may (will likely) need access to an existing email account first to get the new passwords set up.
      - **Your security depends on your hacked account!**
- **TAKE A RISK:** You will take a (hopefully) small risk now. Bigger ones come later.
  - On your Chromebook, log out/off. Then create a new account using your existing critical email address (if you have more than one, create an account for each as you need it).

    - Login to the new account using your pre-existing password and **change the password** to something unlike any previously used password you have ever had.
        - **DO NOT** use this account for any other purpose yet.
        - **USE THE WEB ONLY TO DO THE RESET**: Do not use any apps and do not download your emails. Use the email provider Web interface only.
        - **DO NOT ENABLE ANYTHING OR SAY YES TO ANYTHING ELSE ALONG THE WAY:** The only thing you should need is to get the one password reset email from the Web email interface, to click on the one URL within that email from the provider you requested the password reset from, and to enter a new password for that account at the Web interface.
        - **SWITCH BACK TO THE NEW UID:** On the Chromebook, you can be logged into more than one user identity (UID) at a time. Essentially, you pause using one account and switch to the other. Switch UIDs back to the new clean account.
- **CHANGE YOUR PASSWORDS** on all of these other accounts. It will likely go something like this:
    - From the Chromebook, go to the Web site of the existing account.
    - Tell it to do a password reset. It will likely want to send a reset URL to your previous existing email address.
        - **You will not yet have access to that account unless you already reset that account per the above.**
        - It will (normally) email a reset URL to your existing (hacked) account.
        - **Switch back to the old UID**, get the email, change the password on the critical account.
        - **Switch back to the NEW UID.**
    - Now that you have a **new password** for the critical account, you should be able to login from your **NEW UID**.
        - Login to your critical account from your **NEW UID**.
        - Once logged in, change the password on your critical account again to a **new new password**.
        - **DO NOT USE THE EMAIL RESET THIS TIME**
        - At this point, your **new new password** for your critical account should only have involved interactions with your **NEW UID**.
        - Save the **new new password** for your critical account – if digitally **ONLY FROM YOUR NEW UID**.
        - **DO NOT** use your old passwords or anything like them as your new passwords.
        - **Change the email address** for your critical account to your **NEW UID**.

- Repeat the **CHANGE YOUR PASSWORDS** step until critical accounts are “secured” and usable from the **NEW UID**.

By now you should have control over your critical accounts from your **NEW UID.**

- **DO NOT GO BACK TO YOUR OLD UID FOR THIS CRITICAL STUFF.**
- Now that your critical accounts are completely independent from your old insecure everything, you could remove the **old UID** from your Chromebook and use this system with relative safety moving forward.
- However, you would not (yet) have access to your other stuff.
- If you have the money and want to be more careful moving forward
  - Get a second Chromebook for the less critical stuff and keep the critical stuff on the isolated Chromebook that only does the critical stuff.
  - Don’t load any apps into the isolated Chromebook or use it for any purpose other than the critical stuff.
  - Keep it locked up when not in use and do other similar stuff to secure it.
  - You might want to use the Google backup mechanisms for keeping passwords, etc. so that if the isolated Chromebook breaks (which all things eventually do), you can restore from Google with a minimum of inconvenience.
- **What about my cell phone?**
  - At this point, if you have a cell phone it will have lost access to some of the accounts you changed the passwords for. If you had multi-factor authentication involving that phone, you have been using it along the way (calls or text messages – the email might no longer work because of the password change).
  - **BEFORE YOU CHANGE THE PASSWORDS ON THE CELL PHONE**
    - Consider cleaning out the cell phone as well. You can do this with a “hard reset” or similar “factor reset” of the phone.
      - Then reload the critical things and consider **NOT** including the critical accounts you just reasonably secured.
    - In essence your cell phone is like any other modern 24x7 network connected general purpose computer system.
      - It may have some added security mechanisms over a standard PC running Windows, but it’s not impervious to attacks.

Recover your previous capabilities

SLOWLY gain access to your less critical resources.

Here’s where it gets a bit dicey.

- Everything we bring into the “secured” environment introduces new opportunities for it to become less secured.

- The more we “invest” in a system by adding more of our precious stuff to it, the more likely it is to be hacked again.
  - At some point the extra potential for having to go through this recovery thing again is not worth the added time and effort of putting more stuff into a more secured environment.
- One reason to take it slowly is that some things are used more frequently and are more important sooner, while other things are less important and used less frequently.

The easy (fast, cheap, risky) way:

- One relatively easy thing to do is to go back to your **hacked system**.
  - Reboot it, plug in the **brand new 4Tbyte USB drive**, and copy all of your data to the external drive. Disconnect the USB drive when it finishes (could take 8 hours or more depending on how much stuff there is).
  - Be certain to do an appropriate backup of everything important to you. If you snooze you lose…
  - Note your previously **brand new 4Tbyte USB drive** now contains all sorts of unknown stuff, that could include all sorts of **malware, viruses, corrupt content, and who knows what else**. For that reason, your **brand new 4Tbyte USB drive** is now a **highly dubious collection of possibly unknown content**.
- Then you can “take it back to formula”. Most modern systems have a mechanism to “**restore to factory defaults**”. This will wipe out everything on your computer. Do this to your **hacked system**.
- Once done, your **hacked system** will become a **practically new system**.
- However, as soon as you connect your **practically new system** to your **highly dubious collection of possibly unknown content** it becomes a **questionable at best system**.
- But what the heck – it’s relatively quick, painless, and you can proceed forward from there as and if you like.

The slightly better (less risky, in some ways faster) way:

- In this variation of the theme, you go back to your **hacked system**.
  - Reboot it, plug in the **brand new 4Tbyte USB drive**, and copy all of your data to the external drive. Disconnect the USB drive when it finishes (could take 8 hours or more depending on how much stuff there is).
    - **ONLY BACK UP THE DATA** (usually the files in your home directory)
    - **DO NOT BACKUP THE SOFTWARE OR THE SYSTEM** (much of the malware and the mechanisms that trigger it are usually embedded in parts of the system not containing the user’s content)
    - **WHEN DONE – SAFELY REMOVE THE DISK AND POWER OFF THE COMPUTER**

    - Note your previously **brand new 4Tbyte USB drive** now contains lots of unknown content, that could include some sorts of **malware, viruses, corrupt content, and who knows what else**. For that reason, your **brand new 4Tbyte USB drive** is now a **questionable collection of possibly bad stuff**.
- You should now be able to mount your **questionable collection of possibly bad stuff** on your **not yet highly corrupted Chromebook** and access the content from there.
    - As you slowly and increasingly use your **questionable collection of possibly bad stuff** in your **not yet highly corrupted Chromebook**, the risk increases that your **not yet highly corrupted Chromebook** will, over time, become a **questionable at best system**.
    - You can reduce the odds of your **not yet highly corrupted Chromebook** becoming a **questionable at best system** by using only "trusted" applications from the app store.

At this point, hopefully, you have converted a significant percentage of your digital world into a workable situation. You are reading your email over the Web interface from a system that resists the most common sorts of corruption and allows maximum functionality for minimum personal technical risk.

However, for many people who use high end / purchased software that only runs on a Windows PC, this will not work for some of the important things they own. That's where the "slowly" part starts to come into play.

- The next step is to go back to your hacked system when and if you need it and try to clean it out or take it back to formula.
- That is beyond the scope of this article, but hopefully we got you 80% of the way in 20% of the time and effort.
- Seek professional help at this point… or wait till someone (else?) writes a follow-up.

And then there is everything else…

I just want to take a minute to cover the "everything else". Now that you have been hacked, you should realize that whatever they got has intelligence value beyond the content itself. By reading your emails, seeing your pictures, sending out false tweets, accessing your online accounts, and so forth, they potentially have detailed knowledge of you and your family and friends, including psychological information and triggers they could use against you and your family and friends. You likely cannot change these things, and restoring your systems does not undo this. You have been digitally assaulted and you should address this from many other angles. We have other articles on those subjects, and I am sorry for your loss.

Conclusions

Many years ago, my article on "protecting a poor person's integrity" discussed a now largely outdated approach to keeping individuals safe from bad folks when using the Internet. Things have changed, and so this new version of helping the poor individuals of the world survive in the bad old Internet.

But to be sure, this is a simplistic and partial solution to a far more complex and problematic world we live in today. So be it! Hopefully this will help some folks have better digital lives.

