**The Security Section
Society of American
Archivists**

Protect to Preserve

November 2020
First Encounter

Information, Observations, and Things to Ponder

Secure Your Stuff

- By Jeff Lundgren

What do you get when you Google "secure your stuff?" Among other items, an article in PCWorld.com on locking down your Android phone. Is that all there is to security? Because cell phones (not the flip phone I have) are mobile computers probably more powerful than the main frames that sent Apollo 11 aloft, we all think that's all there is. Could be. But go ahead and let someone hack your phone. Your car will drive itself off the road, your house will be reprogrammed to overheat or shut off the refrigerator and/or allow intruders to, yes, intrude, and your private emails will be sent to someone else's computer. And there's more.

How do we "secure our stuff" in the cyberworld? Thanks to some great information on the security office web page at UC Berkely, here's a primer:

Protect yourself

- Protect yourself beginning with your password. Don't use your screensaver to remember your password or ask a friend to remember it for you!
- Use a long alphanumeric password with as many characters as possible; twenty would be nice. Or use a passphrase with a number-for-letter substitution. For example, "My cat loves squirrels and dolphins" can be converted to "MyCaL0SqAnD0" and do notice the zeros that were added.
- Try biometrics, either with your fingerprint or face ID, for access control to your device
- Use a password manager
- Check regularly to see if you have been breached (https://haveibeenpwned.com/)
- Do not reuse passwords or other credentials-ever!
- Be sure you are using a secure site. Look for the "https://" URL (the one with the "s" for "secure") and a lock icon in your browser
- Avoid public WIFI
- Practice situational awareness and be alert for "shoulder surfers," people who look at keyboards for password information when other users are logging in. Try to locate to a place away from other people or simply be aware of your surroundings

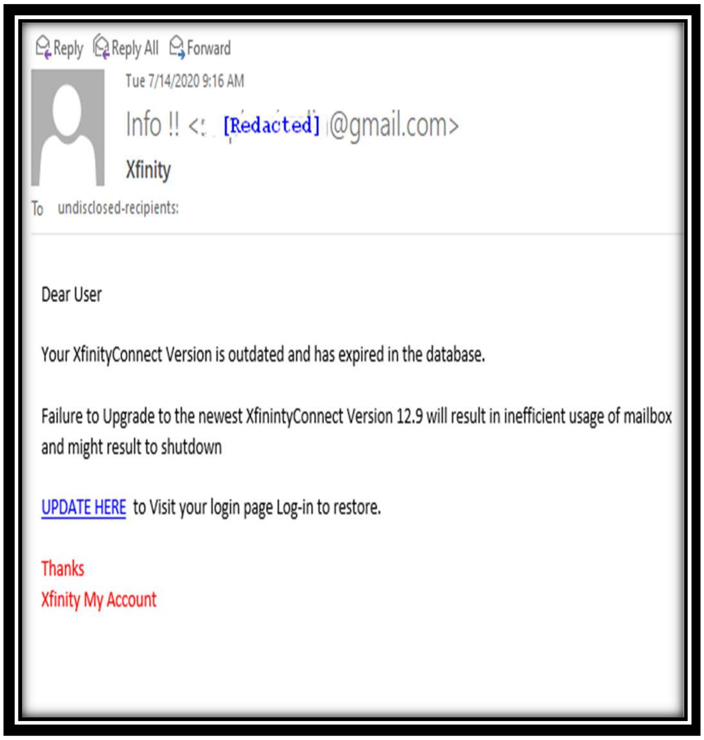
University of California Berkeley. *Security Basics 101*. https://security.berkeley.edu/education-awareness/best-practices-how-tos/security-basics-101

Quote for this Day

"Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are."

--Jeh Johnson, former Secretary of Homeland Security (https://www.dhs.gov/news/2014/02/12/remarks-secretary-homeland-security-jeh-johnson-white-house-cybersecurity-framework)

Let's Go Phishing!



Tue 7/14/2020 9:16 AM

Info !! <: [Redacted] @gmail.com>

Xfinity

To undisclosed-recipients:

Dear User

Your XfinityConnect Version is outdated and has expired in the database.

Failure to Upgrade to the newest XfinityConnect Version 12.9 will result in inefficient usage of mailbox and might result to shutdown

UPDATE HERE to Visit your login page Log-in to restore.

Thanks
Xfinity My Account

Quiz

- By Jeff Lundgren
  (with Jim Havron)

If you have antivirus software, are you and/or your organization protected against malware?

Answer:
According to SecurityToday.com, you will be until you skip updates and regular security scans. Think of maintaining your system in the same way you practice going to the dentist. It's an important item and issues will happen, but they are preventable, if caught early. Antivirus software is the dentist, but if you don't help yourself, it (or he/she) can't help you. Simple, yet doable. So, check it out here: (https://securitytoday.com/articles/2019/04/29/fivebiggest-security-myths-busted.aspx)

Addendum
And while this is true, up to a point, it is best to remember that traditional malware is only a part of what might be added to your computer or system. Ant-virus or anti-malware applications usually work by identifying known patterns. Anti-virus uses a directory of known malicious script, while other anti-malware software might look for specific behavior or types of script that are associated with threats to one's system. Because there are many pieces of dangerous bugs, viruses, Trojan Horses, Worms, and executable files, constantly being designed, refined, rearranged, and redeployed, it is not possible to keep them all in a library where they are recognizable, or even their file type or behavior can be identified as malicious.

Research by security companies and hacker (non-criminal) organizations suggest that even fully updated software will catch, at most, 25% of malicious code that attempts to infiltrate a system's defenses.

So why go through the process of updating the anti-virus? Be assured that 25%, even at most, is a very significant reduction in an attack. Security is usually set up in layers, with different layers designed to stop different types of attack. Ant-virus/anti-malware is one of those layers. Their may be 7-10 layers, so knocking out 25% at one level is that much less that must be defeated on the malware front.

-Addendum by James Havron, CA, Security+, CEH [Certified Ethical Hacker]

Phish! ⌂

The image above is a cropped copy of a real message sent to an individual. The email of the "sender" has been redacted. The "UPDATE HERE" text did hold a link, but it has been rendered inactive by the transfer to a still photographic image.
How many clues can you find that this is not a legitimate message? Can you identify the techniques used to try to persuade the receiver to act as the sender would wish? You may include some assumptions, such as "If the were not received on Tuesday as is shown, it is likely bogus". [Hint: That is NOT a correct assumption, just an example of how one might point to a suspect piece of information as a clue].

This message has some obvious items if one is used to looking for such things, but everyone is not. Please post your ideas on the discussion page for the SAA Security Section, or email them to jimhavron@comcast.net.

Developers, designers, security specialists who design their own tools, hobbyists, "Makers", all make use of sensors of different varieties in their craft.

I began using sensors in projects in the days before the advent of the microprocessor. Thermistors, photodiodes, rh-resistors and capacitors, all part of slightly earlier electronic instrumentation. Generally, there was some measurable change, usually chemical, in components of a circuit, that would be caused by changes in the environment and would cause a change in electric characteristics in that circuit. More than you wanted to know? Well, okay, but it can come in handy if you work with an institution that has no budget for monitoring.

Present sensors will do the same thing as sensors + circuitry would do in the past. They can be used to make very inexpensive, computerized monitors to log changes and send alarms. More than one cultural heritage establishment I work with has standard and infrared cameras triggered by motion, designed not to monitor the reading area during hours, but after hours. There are also such devices in areas of the establishment, including outdoors, where people are not supposed to be at different times, or ever. Some capture images when people handle things they should not (both the "do not handle" instructions and "covered by surveillance cameras" warnings are well posted). Custom made to the individual site, and usually with an extra as backup, they cost a fraction of commercially available devices.

Usually the skills are not worth acquiring just for the sake of providing cheap equipment, but if you know someone who does this type of stuff, or if you want to learn, you can often find people to teach you. Clubs and interest groups abound for hobbyists and makers (these are people who build working devices, often robots, drones, electronic devices to solve problems and do tasks, computers that will serve in place of desktops but with "hot swappable" systems and software, all of which can fit in a pocket), many tech professional groups have people who design and build, as well as develop software, device defenses, devise ways to defeat defenses. Members of archivist, librarian, and other cultural heritage professional organizations may have people who can help. One can reach out to these groups with your needs. The worst they can do is say no.

Anecdote: Some years back, a special collections and archives section of a much larger organization wanted to install a single surveillance camera at the front desk. A single staff member was staying late and alone, and often felt uncomfortable. The larger organization used safety cameras in many different places, requiring high resolution to cover large areas, so it set a standard for any cameras. There was no budget for the camera requested, and even with support from elsewhere there was a need for over $3,500 for the small unit of the building. They instead used a small, custom built motion activated camera. When a person appearing intoxicated and belligerent came in one night, causing the staff member to retreat to the back to call security, the camera was able to capture an identifiable image of the person, as well as the theft of 3 items from a display case that, while not unbelievably valuable on the market, were irreplaceable of of significant historical value. (As an aside, there was still no budget for cameras in the next budget.) Just something to think about.