November 2024

Recent Topics Revisited

By Mark Costlow

This month we are following up on some topics from the past year or so with updates.

1980s Call Screening for iPhones

Remember answering machines? In the really old days, they had cassette tapes and made a bunch of clunking sounds as they rewound to play your messages. Technology always has unintended side effects, and a big one for the old answering machines was that you could listen to the caller leaving their message and decide whether you wanted to pick up the phone or not. Remember, this was before Caller ID and answering the phone was a roll of the dice. It could be a relative, a friend, a politician, or a bill collector. You wouldn't know until you picked up the phone. Call screening with the tape machine became a thing. If you've forgotten what this was like, or never experienced it, watch the first 30 seconds of an **Intro to a Rockford Files episode** for a quick refresher.

In the 2000s, call screening faded away in the face of Caller ID and voice mail systems, but Apple is bringing it back. In iOS 17 and beyond you can watch a live transcription of voice mails left on your phone, and even pick up the call before the hang up if you decide you want to talk.

The feature should be on by default, but if you want to check or turn the feature off, go to **System > Phone > Live Voicemail**. When someone calls and gets sent to your voice mail, a notice should appear on screen that a voicemail is being left. If you tap it you should see a live transcription of what they are saying, and you can tap an option to pick up the call. I don't answer any calls from numbers I don't recognize, so this is a way to catch the few of those which are people I want to hear from.

While you are in the **phone settings**, you can also select "Respond with Text" to set a few canned text messages which you can send in response to someone calling you. "Sorry, can't talk" is the default message, and other useful settings include "On my way" and "I'll call you back".

This only works for English in iOS 17, but supports several other languages as of iOS 18. Some Android phones also **support Live Transcribe**, including the Google Pixel and Samsung Galaxy.

Scammers Still Scamming

Sometimes we sound like a broken record talking about scammers and how careful one should be about responding to any unexpected communication. However, from our vantage point as a place many people report their run-ins with scammers, we can see that two things are constant:

- Scammers never quit. If an individual scammer moves on, there are two more to take its place.
- Scammers evolve. They continuously improve their gambits.

The current trend is using personal data to make scam pitches seem more legitimate. This month we saw a "shame extortion scam" that was very similar to **what we've seen the last few years:** they claim to have control of your webcam and have seen you do something naughty and will send it to your friends and family if you don't send a bitcoin payment. But this one was enhanced with loads of personal information about the targeted person: their phone number, physical home address, and names of friends and family members.

All of this information can be gleaned from some combination of public data and breached data. So many large databases have been breached: **data brokers**, **financial institutions**, **government agencies**, **healthcare giants**, and more. Many of our personal details are now in the hands of criminals, and supercharging scams is one of the ways they are putting it to use. If you receive one of these extortion scams you can report it to the FBI at **https://complaint.ic3.gov**.

One of those data breaches in particular is worth noting. Change Healthcare, part of Optum and a subsidiary of United Healthcare, is one of the largest medical payment processing companies in the world. Their **ransomware breach in early 2024** is of note for three reasons:

- The huge number of people in their database. They have **publicly confirmed** that "the impacted data could cover a substantial proportion of people in America".
- More data leaks are possible. **They paid the criminals a $22 Million ransom**, but have no guarantee they won't continue releasing data (they are criminals, after all).
- The **nature of the leaked data** is particularly useful to scammers. It includes the usual personal details and account numbers, but also medical information: test results, images, prescriptions, procedures, doctors' names, and more.

Visit **https://changecybersupport.com** to keep track of what Change is offering as compensation. It's a good idea to take advantage of the two years of credit monitoring service they provide. One can't help but note that this breach will be affecting people for much longer than two years. It is still a developing situation though, so check back every few months to see what has changed.

Tracking Will Continue

In June and July we looked at privacy, or lack thereof, and how data brokers collect our data and track our movements. One mechanism they use are "**tracking cookies**" - little data tags used by web sites to monitor you as you roam the web.

One effort to curtail this use of cookies was spearheaded by Google, when **they announced in 2020** that they would disallow "third-party cookies" in their Chrome browser. They announced a 2-year timeline to accomplish this change. The **MRS Digital blog** describes the milestones in that project, starting with that initial announcement in 2020, all the way through **Google's disclosure in July 2024 that they have given up**. They will not disallow 3rd-party cookies in Chrome. Users will be able to opt-out of them individually, but no sweeping change to automatically reduce the amount of tracking will happen.

The original **Do Not Track** (DNT) effort began in 2009 aiming to let users opt out of web tracking. Progress has been slow, as there are enormous piles of money at stake. DNT has been superseded by **Global Privacy Control** (GPC), introduced in 2020. GPC is more aligned with privacy laws that have appeared since DNT was introduced such as the **California Consumer Privacy Act** (CCPA). A handful of states have laws similar to the CCPA and the GPC complies with their requirements. The idea is that this will make implementing GPC the easiest way to comply with the law.

The **Didomi Blog** has a comprehensive treatment of Global Privacy Control and lists which US states have consumer-friendly privacy laws.

More Credit To Freeze

The **Cyberhoot Blog** reports that there are actually four major credit agencies, not just three. They recommend freezing your credit at **Innovis**, along with the Big 3 (Equifax, Experian, and Transunion). Innovis has a freeze form on their web site. Cyberhoot mentions some other smaller agencies that you can contact as well, but the law of diminishing returns suggests it may not be worth the effort to go too far beyond the ~~Big 3~~ Big 4.

Generative AI Generates Errors

Generative AI and Large Language Models (LLMs) have been around a little while now, and are seeping into our everyday use at all levels. Studies are coming out which seek to characterize the quality of these tools. Are they as good as advertised? Do they really save time? Are they in fact dangerous?

A study from **Motley Fool** found that a very high percentage of Americans have used ChatGPT, and around half of us have asked it for financial advice, about everything from credit cards to personal loans. As usual the advice is to independently verify any advice you get from a machine before putting it to use.

At the same time, other studies conclude that **LLMs are not good at math**. Part of the problem is the "tokenization" process where input prompts are broken up into words for analysis. Since LLMs don't really know what numbers are, they might arbitrarily accept "250" as a number, but consider "283" to be "28" and "3". It's a very minor textual detail, but a huge difference if you are doing math.

Apple released a widely tracked scholarly report which concludes that LLMs are not good at reasoning. They systematically tested many systems, both public and private, and their conclusions are applicable to Generative AI techniques as a whole, not a specific product or chat bot. They say, "Current LLMs are not capable of genuine logical reasoning [...] Instead, they attempt to replicate the reasoning steps observed in their training data."

The core idea is that LLMs don't really think through a problem. They are good at pattern-matching to find examples of humans previously applying logic to a similar problem. Apple calls this model "fragile" because changing seemingly unimportant things in the query (like only changing the names of things in the question, not the form of the question) can result in very different answers.

It is a little ironic for Apple to be shining this light, while also aggressively promoting the addition of Generative AI in their latest systems.

One success story for LLMs has been computer programming. Many programmers use it with reportedly great success. The **Futurism blog** reports on a study by Uplevel (a management software business) which found that programmers who use **GitHub's Copilot AI** are not more productive than before. They studied the same set of 800 programmers for three months before and after they started using AI, to control for variables like experience levels. The rate of completion of coding tasks was not increased, and the error rate was higher.

Andrew Zuo points out that using AI to develop code for a new or novel system could be dangerous. Since AI excels at finding existing examples in its training data, asking it to create truly new constructs will often result in "hallucination packages". This refers to AI's propensity to offer a solution which uses an external software package to handle some functions, but the package it references simply doesn't exist. It's like winning a trip to London and being told you only have to cover the airfare, hotel fees, and meals.

And finally, **Google announced** that more than 25% of their new code is being generated by AI. Read into that what you will.

The bottom line is LLMs are still relatively new and like many hot new technologies, our expectations will be tempered by reality over time. But the tech will also improve, and studies like these help them do that. One specific improvement I have seen is that a year ago I could not get ChatGPT to write a haiku no matter how hard I tried. It messed up the (extremely simple) format every time, producing doggerel with random numbers of syllables. But the current version of ChatGPT generates 5-7-5 haiku every time, like this one about its previous struggle:

> Buzzing gears at work,
> Syllables slip through its grasp,
> Seven, five… six? Close.

Southwest Cyberport - swcp.com

New Mexico's Expert Internet Service Provider since 1994

505-232-7992* | *Support: help@swcp.com

5021 Indian School NE, Ste. 600, Albuquerque, NM 87110

Click on bold blue type in browser for links.