April 2026

Time to Update Your iPhone (Really)

By Mark Costlow

Google is pretty good at finding security exploits in systems of all types, not just their own phones and tablets. And Apple excels at taking exploit reports seriously, developing fixes for them quickly, and pushing them into iOS updates for their customers to apply.

If only us users were a little better about doing updates. Well, that's not entirely fair. Most of you ARE good about doing updates. But there is a measurable cluster of diehards that are slow to update for a variety of reasons, some good and logical, others whiny and lazy.

For myself, it's a combination of valuing stability (I never run the "dot-zero" release of a new system if I can help it), being hesitant to grapple with new flavor-of-the-week style interface changes, and being too busy to carve out the time or mental energy to deal with a new or changed system.

As of January 2026 there are **2.5 Billion active Apple Devices** in the world. **According to Apple**, almost 60% of them have updated to the latest system, iOS 26, which was launched 6 months ago. To be fair, Android and Windows would love to hit numbers like this.

The latest Android OS, version 16, was released 9 months ago and **has under 10% adoption**. Even if you combine that with Android OS 15 from 2024, **they still have under 30% combined**, which leaves billions of devices running old systems.

Windows 11 has a slightly better coverage than iOS 26 so far, with **about 62% adoption**. The embarrassing part is that Microsoft has been pleading, cajoling, and threatening users for over 4 years to get to this level.

But, even with Apple's remarkable ability to get their user base to stay more current than most, there are still hundreds of millions of devices left running the previous release.

Why Do We Care?

This is not new. Apple has excelled at dragging us into updated software for years, and there are always slow-pokes and hold-outs like yours truly. What has suddenly made this a big deal is the recent leak of the **DarkSword** hacking tool.

We mentioned that Google is good at bug-hunting. The **Google Threat Intelligence Group (GTIG)** started tracking a series of web-based zero-day exploits targeted at iPhones in November, 2025. A zero-day exploit is a security bug that is so new, the makers of the software it targets were unaware of it and therefore have not patched against it. Zero-days are the holy grail of black-hat cyber criminals, and the ones in this story have names like GHOSTBLADE, GHOSTKNIFE, and GHOSTSABER. A black-hat security researcher who finds a new zero-day exploit that works against an up-to-date iPhone **can sell it for millions of dollars**.

Most buyers of zero-days are commercial surveillance providers or nation-state sponsored cyber criminals. A zero-day can be combined with a simple phishing email or SMS or WhatsApp message to infiltrate the phones of dissidents, politicians, and high net-worth individuals.

What the GTIG found in the fall of 2025 was evidence of multiple zero-days being used in a group, apparently **orchestrated by a framework or toolkit**. Further, they showed signs of use by different bad actors, against different targets. Most of the use was outside the US in places like Saudi Arabia, Turkey, Malaysia, and Ukraine.

So not only were multiple very expensive exploits combined into one tool, dubbed DarkSword by GTIG, that tool was apparently in the hands of several different players, not just one. It seems likely this toolkit is being sold as a turnkey exploitation tool, or possibly even CyberCrime-as-a-Service.

Such tools have existed before, and while it is frightening how thoroughly and easily they can dismantle the average person's digital door locks, they are not often used against the masses. The reason is simple: Money. If the tool is used widely, the defenders will quickly detect it, identify the bugs, and report them to the software makers so they can plug the holes.

Someone who paid a million dollars for a zero-day will be careful about who they let use it, to keep the golden goose laying its eggs.

As the GTIG found these exploits, they reported them to Apple, who issued fixes for them relatively quickly. Anyone applying regular software updates on their phones and tablets got fixed and protected. This process plays out every month in our modern world. The GTIG even published a **blog about their DarkSword findings** in in mid March.

What changed the urgency level on this for regular users is someone leaked the DarkSword toolkit in late March. They posted it on **GitHub**, the world's largest site for sharing computer code.

While GitHub may have removed the code after it became known, it was too late to stop the spread. This military-grade cybercrime tool, which is reportedly easy for any programmer to use, is now out in the world and available to be used by **anybody**, not

just nation-states or global crime syndicates.

DarkSword targets iOS 18.3 through 18.7. All of the vulnerabilities have been patched as of iOS 26.3. (iOS 26.4 is the current latest version. We won't go into it here, but iOS renamed itself so that iOS 26 is the next release after iOS 18 ... versions 19 through 25 never existed).

Anyone running iOS 18 because they were worried about the user interface changes in iOS 26 is now out of excuses. We all need to apply that update now. Websites with DarkSword-created exploits on them are proliferating as you read this.

Lest you think you are safe because you are on an even older iOS, know that the lineage of DarkSword has been traced to an earlier tool with apparent Russian ties called **Coruna, which targets iOS versions from 13.0 up to 17.2.1**. It's time to just go to 26.

iOS Settings to Ease the Change

Two of the most common complaints about the iOS 26 "liquid glass" interface, and settings to mitigate them, are:

- The "glassy" transparency, coupled with animations, are distracting. There are 2 settings that can help with this (the "motion" one is new in 26.4). Try them each and see which you prefer. In the Settings App:
  - Older option: `Settings > Accessibility > Display & Text Size > Reduce Transparency`
  - Newer option: `Settings > Accessibility > Motion > Reduce Motion`
- The large time display on the lock screen doesn't look good with transparent numbers:
  - Tap and hold lock screen, then click Customize
  - Swipe to the lock screen you are using, tap the time
  - At the bottom change the selector from "Glass" to "Solid"
  - Click to dismiss the font settings, then click "Done" in the upper right

Luddite Lockdown

If you are in a position where you just can't or won't update to the latest iOS, and are willing to accept some limitations, Apple has a solution for you. It's called Lockdown Mode.

Lockdown Mode provides "extreme protection" and is intended for select individuals who, by virtue of who they are, may be targets of sophisticated and persistent digital attacks. It's made for dissidents, politicians, celebrities, Fortune 50 CEOs, etc.

In Lockdown Mode, many device features are restricted, such as messaging, photo sharing, wireless connections, and more. It will absolutely inconvenience you. The number of phones compromised by DarkSword is already estimated at over 100 million as of this writing, so if you can't update to iOS 26, Lockdown Mode might be a good option.

Closing Thoughts

Isaac Newton famously said, "If I have seen farther, it is by standing on the shoulders of giants." New science and technology is always built on what came before. Our modern software stacks become ever more complex as each generation has more and more capabilities to build upon.

The complexity of interactions within any one of these systems is already incredible, and now that the systems can all talk to each other, there is an explosion of possibilities.

This burst of new abilities is hugely beneficial, but humans are struggling to harness this power safely. AI is being used to slap together new features and subsystems at unprecedented speed, with human experts out of the loop. Meanwhile, dark forces use the same AI systems to find exploitable holes, not just in new systems, but in every existing system already deployed.

We are at an inflection point. New ultra-powerful tools are pushing the limits and the baddies always have the upper hand. The builders' attention and resources are split between creating something useful and exciting vs. making it safe. The destroyers have one goal: find weaknesses in those systems and exploit them before they can be fixed.

Most security researchers they will say "**Defense In Depth**" is the key strategy. That means we don't just do one thing to keep us safe, like install an anti-virus or have good passwords. You do all the things, or as many as you can manage, to keep the criminals at bay.

But if you press those researchers further, to get **one thing** that busy regular people should do to keep their digital lives in tact, most of them would agree (after the password thing): keep your system software updated, especially phones and computers, where it is easiest to do. The army of people making new things with security holes also have platoons working tirelessly to plug those holes and push out the updates. Apply the updates so their efforts are not wasted.

This Month in Ideas & Coffee

- **Apr 21 6pm-7:30pm –** *WordPress Work Along* – Questions, ideas, and conversation about WordPress. Bring your laptop!

Watch the **Ideas & Coffee** event calendar at **https://swcp.com/calendar** for future info.

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.