Artemus Consulting Group

Volume 8, Issue 6
March 19-April 1, 2022

FANS SUMMARY WEEKLY

Good evening, dear FANs. The advent and promise of Spring has finally, FINALLY come to us. That said, this Spring is different than that of previous years. "Why?" you may ask. Well, it is with great displeasure, unbelievable consternation, and even more sadness that I must report to you that Artemus Central, the hub of all things good, the nucleus of amazing content gathering and one of the world's publishing giants...Artemus Central is closing its doors forever.

"Aaaaapril Fools!!!!!"

Whew! Okay, I got that out of my system! **Welcome**, dear friends! Welcome to our seventh issue of the Artemus Consulting Group's "FANs Weekly Summary"! We have a great (aren't they all?) issue for you and hope that you like what you see and read. FAN Arvo Vercamer contributed a fascinating piece that we know you'll love.So, without further ado, let's get this show on the road!

THE BALTICS: CAUGHT BETWEEN A ROCK AND A HARD PLACE

by Arvo Vercamer

Social considerations: A leading fear amongst ethnic Estonians, Latvians and Lithuanians is that after (militarily) subjugating the Ukraine - the Baltic States will most likely be next in line to be invaded by Russia. Since 1944, Moscow has forced/encouraged the resettlement of Russians/ Russian speaking peoples to reside in the Baltic States. In Estonia, close to 25% of the current population of 1.3M people, are primarily ethnic Russians; in Latvia, 26% are ethnic Russians and in Lithuania, about 5% of the nation is comprised of ethnic Russians (historically, ethnic Lithuanians and ethnic Russians in Lithuania have not gotten along well - even during Soviet times).

The standard of living of these Russians expatriates is presently much higher, when compared to that of the Russians in Russia itself. It need be noted that an overwhelming majority of the Russians residing in the Baltic States do not speak the local language, nor can they really converse in English, German, or other western European languages. Language challenges were not a problem, when Moscow ruled the land - but they became highly evident when (ethnic) Russians no longer constituted the privileged/ruling class in the land. Estonia/Latvia/Lithuania are already stretched to the maximum economically and financially, as well as not having the available housing, medical and daily subsistence facilities to share with the Ukrainian refugees. In Estonia, the arriving children of Ukrainian refugee families had to be quickly relocated to "Estonian-language" schools - at Russian-language schools, the Russian children often started getting violently physical with the newly arriving Ukrainian school children. Long-time ethnic Russian residents living in the Baltic States are very angry with the newly arriving Ukrainians, as the Baltic governments are giving the Ukrainians higher priorities for food, housing, medical services, employment opportunities, etc. Russians residing in the Baltic States still feel like they are bottom-class citizens.

VERCAMER, continued

As of 24 February 2022, Estonia has absorbed over 21K refugees from the Ukraine, Latvia has taken in 9K Ukrainian refugees and Lithuania has accepted over 27K Ukrainian refugees. According to United Nations estimates, 3.1M Ukrainian refugees have so far arrived in Western Europe, the European Union (EU) – and more Ukrainian refugees are expected as the fighting intensifies.

In Estonia (as in Latvia and Lithuania), many local inhabitants are already working hard/planning to seek safety/shelter elsewhere. Relocating to within the European Community (EU) is the preferred option of choice, as opposed to seeking safety with non-EU neighbors. That said, nearly every citizen (of non-Russian heritage) is also resigned to living through yet another Russian occupation - should that happen. By the time the need to quickly skedaddle arrives, Russia will already have control of the Baltics, control of all viable escape routes. Too many native Baltic citizens still remember all-too-well the last two times the Soviets/Russians were in their homelands (1940-1941 and 1944-1991) – and how the Russians governed. Language wise, the younger generations have better fluency in English than do older generations.

Defensive considerations: Overall, all three of the Baltic States are militarily very weak. Since regaining independence in 1991, they have worked hard to fully integrate themselves with the economies of Western Europe, many of the world's leading economic "superpowers", including joining the NATO defensive alliance. The defense ministers of Estonia, Latvia, and Lithuania (Kalle LAANET (EST), Artis PABRIKS (LAT), and Arvydas ANUSAUSKAS (LIT) issued a joint statement after a meeting in Kaunas, Lithuania, on 21 December 2021, called for a joint approach "to counter Russian and Belarussian (!) attempts to destabilize European security."

In defensive terms, the Estonian "active duty army" is presently about 33k in size (army/navy/air force), with about 105k reservists being available for call-up. The few available defensive weapons, however, are not up to the task of defending Estonia from a global nuclear power –Russia.

Russia has made it clearly known that it dreams of a "resurrected Soviet Union/Russian Empire". The crushing of the Prague Spring in 1968, the Hungarian Revolution of 1956, the Soviet-era, the mass deportations to gulags in Siberia, the brutal crackdowns on the postwar resistance movement, the inability to defend themselves, and the ever present threat of being abducted on the street by a KGB van that looked like a bread or mail delivery truck – all these points are vividly still remembered.

The challenge presently facing Estonia is that (theoretically!), the Russian Army could cross the Estonian-Russian border and reach the capital city of Tallinn within a matter of hours. By the time the Estonian army could be fully activated, all of the important Estonian military and economic centers could already be under Russian control.

Two important factors are presently in Estonia's (and Latvia's and Lithuania's) favor:

1.) All three nations are full members of the EU and NATO; NATO troops are stationed on Baltic soil, including U.S. forces.

2.) Recent Russian military operations in the Ukraine do not bode well for the offensive military capabilities and combat prowess of the Russian military to authoritatively and rapidly move into the Baltic States.

Arvo L. VERCAMER is a planetary renowned author and technical illustrator specializing in the field of military history. Arvo and his (British) research partner have also designed a set of postal stamps commissioned by the order of Her Majesty, Queen Elizabeth II, of England. Arvo's written and artistic contributions can be found in, but not limited to, internationally distributed publications such as: Cross & Cockade International, Windsock International, the Dutch-language book "Fokker G-1", the Estonian language books "Põhjakotkad" and "Põhjakotkad 2" (Northern Eagles), the Polish-language maritime history journal "Okrety Wojenne", www.militaar.net, among other specialty military history publications.

HOW TO LOCK DOWN YOUR DATA AND ENHANCE PRIVACY ON IPHONE AND IPAD

contributed by Artemus FAN, Steve Page

Apple's devices, and particularly its iPhone and iPad, feature some of the strongest privacy protections available in an easy consumer product. However, there's more you can do to lock down the data on your Apple devices — here's how.

The iPhone and iPad both feature a number of privacy and security protections built into their hardware and software. A lot of these options and settings are configurable, and while Apple's defaults maintain a good level of privacy, you can further protect your data from prying eyes with the following tips.

Device privacy and security
A private device is only as strong as its security. It doesn't matter how locked down your app data is if a third party can simply pick up your device, open it, and read through your messages, browsing history, and more. Because of that, ensuring your device is secure is a good first step.

Set a strong passcode & use biometrics
The data on your iPhone is only as safe as your passcode. We strongly recommend that you set up a six-digit passcode at the very least that isn't all zeroes or "123456."

It's estimated that a four-digit iPhone passcode takes about seven minutes to brute force. By contrast, a six-digit passcode takes about 11 hours — a marked improvement.

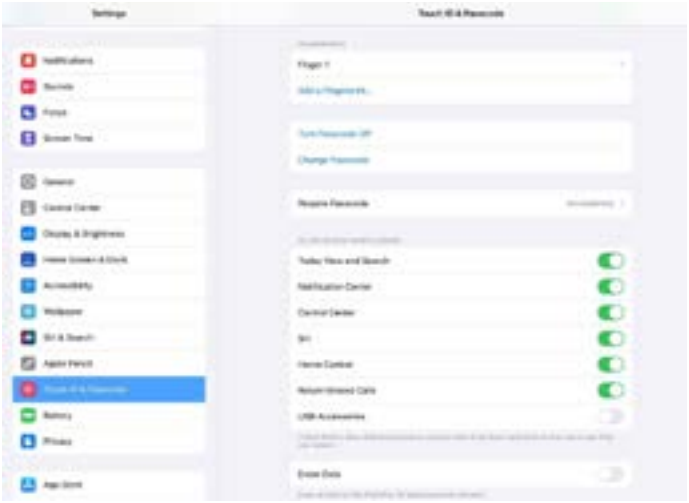
Of course, an alphanumeric password is even better. An eight-digit passcode could take as long as 46 days to break, while a 10-digit passcode could take more than 12 years.

If you find yourself annoyed that you have to type in such a long passcode to get into your iPhone, make sure to enable either Touch ID or Face ID.

Apple has said that Face ID is much more secure than its fingerprint-based counterpart. However, both provide good security compared to shorter passcodes, and they both make longer passcodes more convenient to use.

Additionally, it's understood that law enforcement can't compel users to give up their biometric information — unlike passcodes.

Your strong passcode will not do much if someone can pick up your device and read message previews from the Lock Screen. Although disabled by default on some iPhones, this setting can be manually toggled by heading to Settings > Notifications > Show Previews



The same goes for other data accessible when your device is locked — such as Widgets. While Apple's widgets automatically blank out when a device is locked, other widgets could reveal private information.

You can change the widget Lock Screen settings by heading to Settings > Face ID & Passcode. Scroll down to Allow Access When Locked and disable the toggle next to Today View, Search, and any other data points you'd like to hide when your device is locked.

USB connections
Technically, the toggle to allow USB accessories when a device is locked is part of the "Allow Access When Locked" settings mentioned earlier. However, it's worth a separate mention because

of the security implications.

The feature allows users to protect their devices against sketchy or questionable USB-based accessories. An added benefit is that USB Restricted Mode is also another layer of protection against USB iPhone cracking tools like those made by GrayKey.

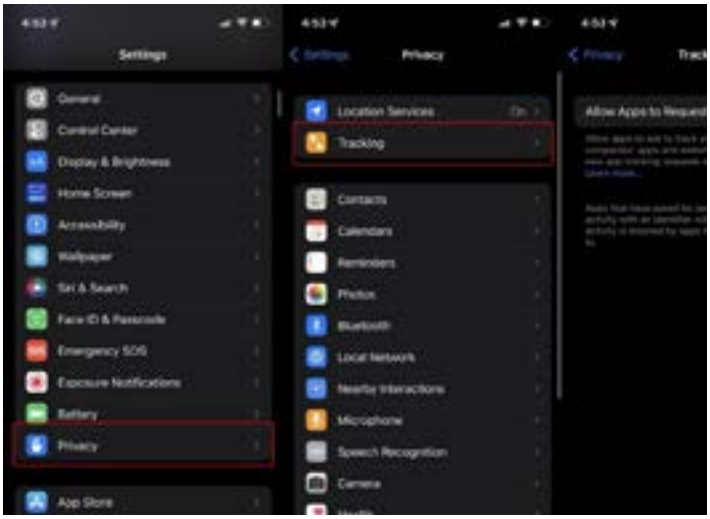
So, even if you don't mind widgets showing on a locked device, it's typically a good idea to disable USB Accessories under the Allow Access When Locked menu.

Make sure Find My is enabled
The Find My network isn't just a handy way to find missing devices — it's also a powerful tool for securing your iPhone. If you enable Find My on a device, you'll be able to track and locate a lost iPhone or iPad using Apple's vast network of connected products.

More importantly, in the context of security and privacy, the Find My app will allow you to remotely wipe your device if it falls into the wrong hands. While not a typical scenario, it can offer peace of mind if you're concerned about someone having physical access to a lost iPhone or iPad.

Data privacy
Once your device is secure, you can move on to making sure your data is private from third parties, whether within an app or using Apple's own first-party platforms.

Turn on App Tracking Transparency
One of the best new features of Apple's iOS and iPadOS platforms is App Tracking Transparency. It essentially blocks apps from tracking you across other websites and services — and it's so effective that Facebook launched a full ad campaign to protest it.



There's a good chance that you've already seen a popup for App Tracking Transparency while using your iPhone normally. However, you can always manage your tracking preferences by heading to Settings > Privacy > Tracking

By disabling tracking for specific apps — or stopping all tracking on your device — you are preventing apps from tracking your online behavior across other apps and websites. That makes it harder to follow you around the web and monitor your online habits.

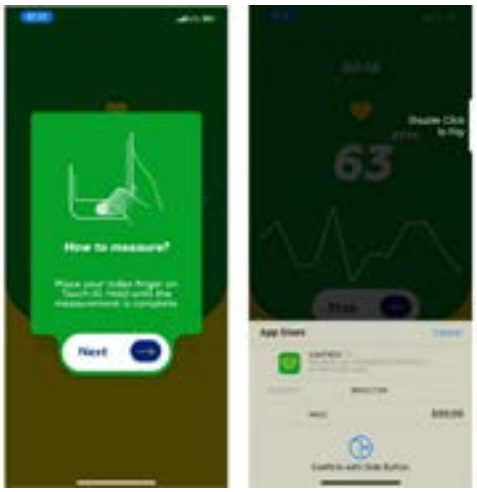
Manage your permissions
Apps can gain a lot of different device permissions by just asking you. You've likely accepted some of these permissions without thinking twice about it. However, there's the potential for apps to abuse these permissions. For example, it used to be possible for apps to spy on users with camera permissions.

These types of attacks and invasions of privacy are rare, but they can happen.

You can review app permissions in Settings > Privacy. It's recommended that you at least take a look at Location Services and disable apps that don't need to know where you are. That's especially true for Precise Location, which means an app would have an exact location of where you are instead of an approximate one.

In the Privacy pane, you can also manage permissions for the microphone, camera, health data, photo access, and more.

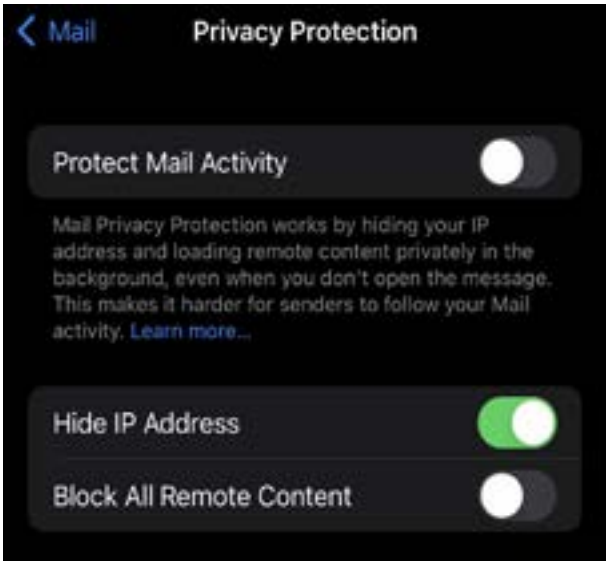
Delete unused (or untrustworthy apps)
Generally, you shouldn't download apps unless you fully trust the developer. While Apple's App Store review team does a good job of weeding out sketchy or malicious apps, some shadier apps do slip through the cracks occasionally.



Scam apps can include "fleeceware apps" that charge high recurring subscription fees after a free trial period. Scam VPN apps could potentially steal your data, while other apps have used nefarious techniques to steal money.

These types of apps aren't as prevalent on the App Store as on Android, but it's still important to maintain vigilance. And, if you care about your privacy and security, it goes without saying that you should avoid installing any profiles on your iPhone that allow side-loading (or app downloads from outside the App Store).

Enable privacy in Mail
If you receive an email from a large company, there's a good chance that the message contains a tracking pixel that can reveal details about your emailing habits — including if you opened a message. A tracking pixel is a tiny graphic virtually invisible to the naked eye that can provide companies with a wealth of data about you.



In iOS 15, Apple has introduced a new feature that can put an end to tracking pixels. Just head to Settings > Mail > Privacy Protection and tap the toggle next to Protect Mail Activity.

Other privacy tips
In addition to device security and data privacy, there are a few additional things you can do to lock down your device and online presence.

Review Apple's privacy access
Managing app permissions and privacy settings for third-party apps is one thing, but depending on how trusting you are of Apple itself, you may want to review Apple-specific privacy settings.

Some examples include Apple's own personalized advertising services. Apple may also collect some data to improve its user experience, including iPhone and Apple Watch analytics data with diagnostic and usage information. Your Siri settings could also mean that Apple is storing and reviewing audio recordings of your interactions with Siri.

If you don't want any of this happening, head back to Settings > Privacy and scroll down to the bottom. Here, you'll see Analytics & Improvements and Apple Advertising. Change the settings as you see fit.

Wipe your EXIF data
By default, your iPhone will record the exact location where photos and videos are taken. This is normally innocuous and allows you to see a map of image and video locations in the Photos app. However, this metadata can potentially reveal where you live, work, and go to school if it falls into the wrong hands. There are a couple of ways to get around this. The first is to remove the location data, which is done in the Photos app. Tap on an image, tap the "I" icon, tap Adjust, and then tap on No Location.

If you like the Photos mapping feature, you can also wipe this data while sending. If you're selecting images to send in the Photos app, tap on the blue Options button underneath the number of photos you have selected. Tap the toggle next to Location.

Use strong passwords
Similar to the passcode on your iPhone, a lot of sensitive data is protected by the password on your online accounts. We recommend using a password manager and making sure each account is secured by a strong and unique password. If you don't want to pay for a separate password service, Apple has its own password manager built into its platforms. The next time you sign up for an account on your iPhone, you'll likely notice a "Use Strong Password" option. If you select that, your iPhone will choose a password for you and save it to iCloud Keychain for later use.

The iCloud Keychain platform is easy to use and a great alternative to a paid password manager for users who own multiple Apple products.

THE COOLEST URBAN DESIGN IDEAS FROM ALL OVER THE WORLD...PART QUATTRO

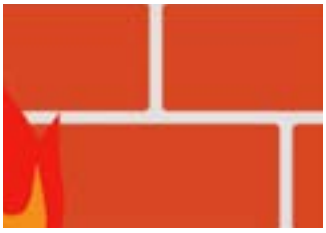
Self-cleaning roads

It's well-known that South Korea is one of the leading countries of the world in innovation. However, this is something that might surprise many of us: water sprayers incorporated into roads. They don't just clean the surface of the roads but also regulate their temperature in order to prevent them from cracking.

Some chuckles from our own Steve Jones...

THIS WEEK IN THE ARTEMUS WEBSITE'S *ARTEMUS SPOTLIGHTS*

[Could we engineer a vehicle with a nearly limitless power]



[Firewall: Definition, technology and facts]

['Really alarming': the rise of smart cameras...]

[Russian hackers targeted NATO...]

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

Thanks for reading! We hope that you found this issue to be interesting as well as a good reference! See you in a couple of weeks.