BIZ NET
BUSINESS - NETWORKS

THE Tech chronicle
August 2019

Recent Popular Aged Face APP on Facebook Has Serious Privacy Issues

If you spend any time at all on social media, you've probably seen the latest craze: People posting photos of themselves aged, so they look like they're in their sixties, seventies, or even older than that. FaceApp, the program behind the face-aging magic has actually been available for a few years, but it has only recently gained the attention of the masses, suddenly and inexplicably going viral after enjoying a quiet existence early on.

Unfortunately, one feature of the app, paired with the company's expansive terms of service could make a number of users uncomfortable.

Let's start with the company's terms of service, which reads, in part, as follows: "You grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you. When you post or otherwise share User Content on or through our Services, you understand that your User Content and any associated information (such as your Username, location or profile photo) will be visible to the public."

That's quite a mouthful but think for a moment about the scope and scale of the permission you're giving to this app to use it.

Now pair that with the fact that when you tap a photograph in the app and instruct it to age you, it uploads a copy of your photo to servers located in Russia. Also note that it doesn't ask your permission to do this, or inform you of it, it just happens in the background.

According to a company spokesperson, the purpose of this functionality is to enhance and improve the speed of the image transformation in-app, relying in part on AI algorithms on the company's servers.

(Continued on next page)

BIZ-NET
1325 Airmotive Way Suite 208
Reno, NV 89502

www.biz-net.com

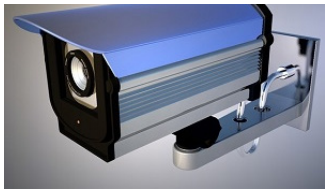
This monthly publication provided courtesy of Marco Romero, President of Biz-Net, Reno NV

Our Mission: To provide the best possible service for our clients using the best tools available today. *As a business owner, I know you do not have time to waste on technical and operational issues. That's where we shine!*

Face APP (Cont.)
It's a (barely) plausible explanation but think about those two things taken together and ask yourself if you're really 100% comfortable with giving that level of control to a company. Is it worth what you're getting in return? For a few chuckles of appreciation at your magically aged photograph?

Most people aren't comfortable with that, but sadly, most people don't read TOS agreements closely before agreeing to their terms. If you're one of the legions of recent fans of FaceApp, keep the details above in mind and discontinue using the application right away.

Update Any Nest Cam Security Cameras You May Own



Did you get your Google Nest Security Camera system used or second hand? If you did, be sure your cameras are running the latest firmware.

Recently, the tech review site Wirecutter reported that some older Nest cams allowed their former owners to access camera feeds, even after the devices had been reset to factory settings.

This is an interesting case because in this instance, the bug wasn't found by a group of savvy researchers, but by a Facebook group for Wink smart hub owners. By pure happenstance and experimentation, the group discovered that feeds from formerly owned cameras could still be accessed via the Wink hub, even in cases where those devices had been reset to factory defaults. This naturally created a buzz, which was picked up by Wirecutter's staff and then promptly forwarded onto Google.

For their part, Google responded quickly, issuing a security patch and pushing it to all Nest cameras connected to the web. Of course, that didn't capture all the Nest cameras in existence. If you've been considering buying some (even from a respected seller like Amazon), the first thing you should do is to check the firmware version of the camera you get and update to the latest if it's not already installed.

Google is better than most of the companies selling smart devices, many of which don't offer any sort of security at all. Even so, as this incident clearly highlights that even Google's firmware isn't perfect.

Given the recent explosion in smart devices in recent years, we can expect to see many more incidents and reports like these. While the Internet of Things holds great promise, it also carries grave risks that should not be underestimated or discounted. If you've embraced smart home culture, be careful.

FACT FILE

DID YOU KNOW?

THIS MONTH IN HISTORY

August 9, 1898
Rudolf Diesel was awarded the patent 608,845 for his diesel internal combustion engine.

August 10, 1966
The first lunar orbiter is launched with its mission to take photos of possible landing sites for Apollo missions in the future. It was aptly named, "Lunar Orbiter I".

August 3, 1977
Radio Shack revealed its first personal computer, the TRS-80 Model I. It came equipped with cassette tape storage, 4KB of RAM and a BASIC interpreter. The TRS-80 was one of the first personal computers to be mass-marketed.

August 9, 1991
The first e-mail was sent from space by astronauts aboard the Space Shuttle Atlantis. They used an Apple Macintosh Portable computer with AppleLink online service. The message contained a greeting from the crew and told that they were having a great time and promised to be back.

August 24, 1995
Windows 95 goes on sale and it went on to sell much more than expected, due to being the biggest product campaign launch in history.

Virtual Private Networks (VPNs)

You may find yourself needing to use public Wi-Fi for Internet access when you are away from home, such as when you are at your local restaurant or coffee shop, or when you are traveling at a hotel or airport. But how secure are these public networks and who is watching or recording what you are doing online? Perhaps you do not even trust your ISP (Internet Service Provider) at home and want to be sure they can't monitor what you do online.

Protect your online activities and privacy with something called a VPN (Virtual Private Network). A VPN is a technology that creates a private, encrypted tunnel for your online activity making it much more difficult for anyone to watch or monitor what you are doing online. In addition, a VPN helps hide your location, making it much harder for websites you visit to determine where you are located.

How Does It Work?

A VPN works by creating a private, encrypted tunnel to a VPN provider that you select. All your online activity goes through this tunnel, then leaves your VPN provider's network to your intended destination. For example, if you're based in Tampa, Florida and you connect to a VPN server in Munich, Germany, any website you connect to will think you are connecting from Munich, Germany. A VPN is simple to use. The first step is finding a VPN provider you trust and then creating an account with them (this usually requires you purchasing their service). Once you have an account, you download, install, and configure their VPN software. Once installed and configured, you connect to the Internet as you always do. The VPN software will silently create your encrypted tunnel and start protecting your privacy without you even realizing it.

Selecting a VPN Provider

Your online activities are only as secure and private as your VPN provider. Be sure to select one that you can trust. Here are key points when selecting a VPN service provider:

- **Logging:** Look for a service which does not keep any logs and focuses on privacy. If your VPN service provider does not collect any logs, it is much harder for anyone to go back and see what you have done online.
- **Where the Company is Based:** Different VPN providers are based in different countries. Be sure you select a VPN provider that is based in a country that has strong privacy laws. VPN providers located in countries that have very few or weak privacy laws may be forced to give up information they collect on you.
- **Servers:** Look for a VPN service that has the servers located in the countries or cities you need. Some VPN providers have thousands of servers and locations across the globe. Do you have a need to make your connections appear like they are coming from a specific country? Can the VPN provider provide that?
- **Compatibility:** Look for services that work across different computers and mobile devices. For example, you may use a Windows laptop, a tablet, and an iPhone. You'll want a VPN service that will work on all those devices.
- **Avoid Free:** Be very cautious of "free" VPN services; how are they making money and staying in business? Free services may collect and sell your information.

A VPN is a fantastic way to help protect your online privacy. However, a VPN does nothing to secure your computer, devices, or online accounts. Even if you are using a VPN, be sure you always follow basic security steps, including ensuring your devices are updated, using a screen lock, and using strong, unique passwords for all your accounts.

WHEN SECURITY GETS PERSONAL

At the center of security efforts, we find personally identifiable information (PII)—the assets which organizations all over the world are entrusted to protect.

What is PII?

The most generic definition of **PII is any information that could be used to distinguish or trace an individual's identity**. Examples include: full names, date and place of birth, and Social Security or national ID numbers, as well as medical, educational, financial, and employment information.

Do all countries in the world recognize PII?

***Technically*, yes**. At least most of them do, but the term "PII" is specific to the United States. The EU, for example, refers to this type of sensitive info as "personal data". Both Australia and Japan simply call it "personal information". **Regardless of the term, the concept is the same: highly sensitive data that requires protection.**

What do cybercriminals do with stolen data?

You've likely heard the stories of major data breaches that expose the personal information of millions of people. Perhaps you've even been a victim of this. But what actually happens to exposed data? How do cybercriminals actually use the data?

They sell it on the dark web. Credit card numbers, national ID numbers, email addresses, and passwords all fetch certain prices on the underground economy.

They launch spear phishing campaigns. With enough information, cybercriminals increase their chances of successful phishing attacks because they're able to target specific individuals or organizations while sounding legitimate.

They pretend to be you. Identity theft is a top concern. If attackers gain access to your personal info, they can open accounts in your name, attempt to claim tax refunds, and file insurance claims, etc.

They attack even more accounts. In the case of stolen usernames and passwords, criminals use "credential stuffing," which is an automated attack using those same usernames and passwords to gain access to other accounts.

What's your role in protecting PII?

First and foremost, always follow our organization's policies, which were designed to protect sensitive data. Stay alert, treat all requests for sensitive data with skepticism, never allow someone to use your credentials (physical or digital) for any reason, and think before you click. If you see something or hear something, say something! Reporting incidents ASAP is a vital part of protecting data.