

# SUPERCOM COMPUTER CLUB TECH TIMES

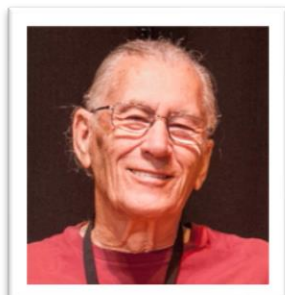
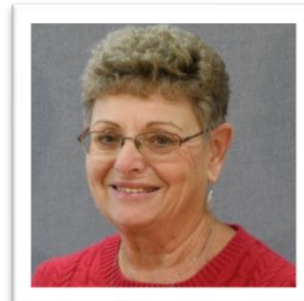
Volume 21    October 4, 2018

## Objective:

To bring the latest technology news to you, our members. Tips and suggestions will help you to keep your device(s) running smoothly and help you be aware of threats. Technical tips will be coming to you through our Technical Committee.

## Committee Members: (Pictured Below)

Ben Tarbell, Mike Gerkin, Peggy Bullock, Jim Mills, Rick Heesen, Lowell Lee, Steve Andreasen (Apple/Mac) and Mike Smith. Jim Oliver and Dick Strong.



Dick Strong and Jim Oliver are on "time off" for season 2017-2018.

Can you believe it?? I am back in Arizona and many of you hopefully will be right behind me. Hoping you are all rested from your “Summer Vacation” and ready to get active in the activities at SuperSun or the SuperCom Computer Club. That’s right – the new season begins the first Friday in November. As I walked down the hall of the club house yesterday, it seemed like I just left! There is that “home” feeling coming back here. The weather has cooled down just in time for you all to get here & enjoy all the activities. Have a safe trip back whenever you head this way!

This will be the last Tech Times for the 2017-2018 Season. Don’t forget to check out the Website.

A couple new Tech Tips have been added from Mike Gerkin –

[Annoying Notification Area Pop-up Messages](#)

[Sign-In or By-Pass Beginning Screen on Windows 10](#)

Remember – Our Club Website is: [www.supercomcc.org](http://www.supercomcc.org).

**All links in our newsletter are safe to click on.**

---

## **Submitted by Art Rice:**

Personalize your PC with these tips. | [View as webpage](#)



[Microsoft Tips](#)



## **Get what you want from your PC**

Learn more about enhanced security measures, time-saving shortcuts, and fun ways to express your individuality.

This is the second in a two-part series. Here's [part one](#).

---

## Keep your PC secure



### Defend your device

Avoid viruses and security threats. Run a security scan with Windows Defender.

[PROTECT YOUR PC >](#)



### Back up your backup

Restore files and schedule automatic backups with Windows 10.

[SET UP YOUR BACKUP >](#)



### Use it, don't lose it

Rest easy with Find my device. Locate and remotely lock a lost or stolen device.

[USE FIND MY DEVICE >](#)



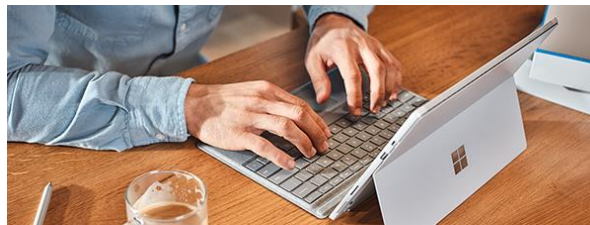
### Sign in with a smile

Hello PC, goodbye password! With Windows Hello<sup>1</sup>, log in using your camera or fingerprint reader.

[SET UP WINDOWS HELLO >](#)

---

### Take a shortcut





### Save time with suggestions

Let text suggestions fill in the blanks in real time as you type.

[SET UP TEXT SUGGESTIONS >](#)



### Speak up

Dictation<sup>2</sup> efficiently turns your spoken thoughts to text.

[DISCOVER DICTATION >](#)



### Type like the wind

There are 150+ keyboard shortcuts for Windows—can you learn them all?

[LEARN KEYBOARD SHORTCUTS >](#)



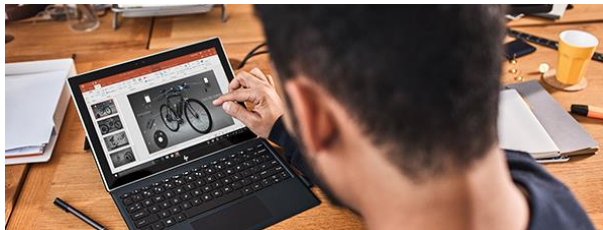
### Show, don't tell

Any shape, any size—with Snipping Tool, it's never been easier to capture a screen image.

[CAPTURE WITH SNIPPING TOOL >](#)

---

## Express yourself



### Your account, your picture

Pick your favorite portrait and set it as your Microsoft account picture.

[PERSONALIZE YOUR PHOTO >](#)



### At a loss for words? 🗨️

Some things are better said with emojis—use emoji keyboard. 😊

[EASILY ACCESS EMOJIS >](#)



### Practice your editing skills

Edit and enhance photos like a pro with easy, fun tools in Microsoft Photos.

[GET FAMILIAR WITH PHOTOS >](#)



### You're the director

Create and edit videos with your pics in Microsoft Photos.

[LEARN HOW TO MAKE VIDEOS >](#)

---

**Submitted by Rick Heesen:**

## **Facebook is Using Your Phone Number to Target Ads and You Can't Stop It**



[Lowell Heddings](#) [@lowellheddings](#)

September 28th, 2018



Tech publications are screaming today that giving Facebook your phone number for 2FA allows them to target you for ads. But this misses a bigger point: Facebook is using your phone number to target ads whether you give it to them willingly or not.

In fact, the problem gets much worse. Researchers have been able to prove that Facebook allows personally identifiable information, like your phone number, to be used to target you based on shadow profiles of information that they build—profiles that you cannot see and have no control over.

So yes, if you give your phone number to Facebook to help secure your account, Facebook will also use it to target you for ads. But if you *don't* give them your phone number, they will still use your phone number to target you for ads. And there's nothing you can do (except delete Facebook).

## What's This Now?

**Control + Click on the title to finish reading the article.**

**You might want to keep up on all the news regarding Facebook if you are a regular user of this app. Just recently 50 Million people's accounts got hacked!!! Were you one? Keep those passwords changed regularly!!!**

---

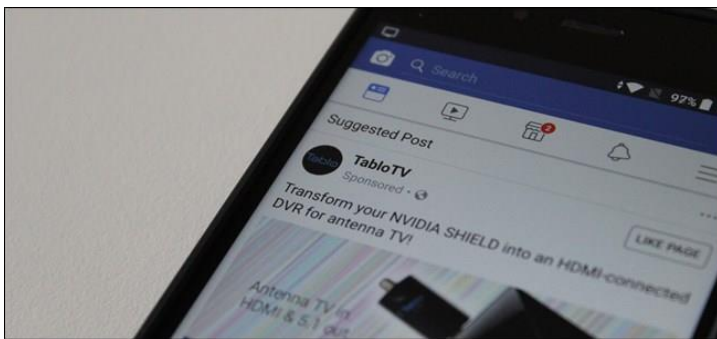
**Submitted by Rick Heesen:**

## [How to Opt Out of Targeted Ads Around the Web](#)



[Cameron Summerson](#) [@Summerson](#)

February 5th, 2018



You've spent some time researching a product on your phone, then you open your laptop and find ads for that product plastered all over the place. This has happened to everyone—it's called targeted advertising, and there are steps you can take to reduce its effect on you.

## What Is Targeted Advertising?

You can probably assume as much by its name, but [targeted advertising](#) is a way for advertisers to target potential consumers based on a number of factors. These include race, sex, age, level of education, income level, employment, economic status, personality, attitudes, opinions, lifestyle, and other interests. Yeah, it gets pretty detailed.

But wait, it gets even deeper. There are various types of targeted advertising: search engine, social, mobile, content, time, technical, sociodemographic, geographical/location-based, behavioral, and retargeting.

**Control + Click on the blue title link to finish reading the article & directions on How to Opt Out**



**Submitted by Peggy Bullock:**

## **[What to do now because of the Facebook hack](#)**

By Francis Navarro, Komando.com

19,581



Last week, news broke out that hackers exploited a flaw in Facebook's code that then allowed them to steal the access tokens of around 50 million accounts, [the largest data heist in the company's history](#).

According to Facebook, the flaw allowed the attackers to use a video uploading feature to exploit Facebook's "View As" tool, a feature that lets you preview your profile as it appears to another user or to the public.

They then used this bug to siphon out the access tokens of millions of unsuspecting Facebook users.

### **Were you logged out of your account last week?**

Out of precaution, Facebook had to log out around 90 million users to reset their access tokens, including users who used the View As feature in the past year.

Although Facebook said that it already notified law enforcement officials and patched the vulnerability, who can say for sure that the issue is resolved? No one knows the full extent of the breach -- not even Facebook itself, it seems.

It's important to understand that as Facebook investigates, it may uncover that more accounts were caught up in the hack. Keep an on eye on your Facebook account, or better yet, follow the steps that we have outlined below for your safety.

### **If you got this email, the hackers have your login account and password**

The Facebook hackers got Kim's information, too.

(Image not available)

This is an email you're going to see if your information got grabbed in the hack. Note that Kim is being allowed to log in with a tap. If you get any similar-looking emails that require you to send any information, they might be email attackers taking advantage of this crisis to steal your information.

**Be careful!**

## What are Facebook access tokens?

Facebook confirmed that the attackers managed to steal user "access tokens" and with these, they can use the affected accounts as if they were their own.

What are access tokens anyway? Access tokens keep you logged into your Facebook account on your gadgets over long stretches of time without having to re-verify your password. It's like leaving your house keys under the doormat, so to speak.

Not only that, but these access tokens are also used by applications and web sites that you linked your Facebook account with. For example, have you ever signed up and logged in to services like Spotify and Airbnb with just your Facebook account? That's your access tokens at work! However, this means that the scope of the breach can be potentially larger since these tokens can be used to access third-party services beyond Facebook itself.

That means that attackers can use your Facebook information to sign in to Spotify, Airbnb, Instagram and any other Facebook-connected app or service and have complete access to those too.

And this may just be the tip of the iceberg. Facebook said that the investigation has just started and there could potentially be more affected profiles.

"If we find more affected accounts, we will immediately reset their access tokens," Facebook said in a statement.

## What you need to do now

If you were one of users who were automatically logged out these past few days, you can still log back into Facebook with your old password. Once in, there will be a banner on your News Feed titled "An important security update." This message will provide you a link that will provide you with more details about the breach.

## Log out of all your Facebook sessions

**Important:** If you were not affected (yet), you should still be cautious about your Facebook account. As a precaution, it is recommended that you log out of your Facebook account on all your devices to reset your old access tokens.

Here's how to log out of all your Facebook sessions.

**Control + Click to finish reading the complete article – KEEP YOURSELF SAFE!!**

.....

**Submitted by Mike Gerkin:**

## Win 1809:

This week Microsoft began releasing its semi-annual major Windows 10 update - Win 1809. Some Windows Insider users have already seen some of the features that have been added or deleted. It has been noted that some users have seen data deleted or system compatibility issues arise.

Considering that some of us have upgrade quite old computers to use Windows 10, it should not be surprising that we may experience compatibility issues with old drivers or features that have simply reached the end of their life and this means they may not work with a further updated Windows 10.

Because of that potential risk being more likely with this major 1809 Windows update, I would strongly suggest that you consider doing a full image backup BEFORE you update Windows 10 to the 1809 version. This action will permit you to revert to a working version of Windows if you actually do run into a compatibility issue, especially on older computers. This would also buy you some valuable time as you consider getting a newer computer if needed.

---

**Submitted by Peggy Bullock:**

As a user of LastPass, I received an email from them today with some good tips. Just thought I would share some of the email.

## Be CyberAware this month

October is **National Cybersecurity Awareness Month** — and it's a great reminder to review and improve your online habits. Because whether you're at home, work, or on the go, staying safe online is becoming increasingly harder. So, to help you get started, we've compiled a few tips:

### Generate random passwords

Unique, randomly generated passwords are the strongest passwords.



### Give email extra attention

Email is the gateway to your digital life. Change your password often, be wary of unknown senders, and don't open unexpected attachments.

## Safeguard your credit



Generate and frequently change passwords for all financial accounts.

---

Your Techs for this time:

Mike Gerkin, Art Rice, Rick Heesen, and Peggy Bullock

Ever notice, the older we get,  
the more we're like computers ?



We start out with lots of  
MEMORY and DRIVE  
then we become outdated,  
and eventually have to get  
our parts replaced...;)

