

## Banking Won't Be The Same After COVID19 - What You Need To Know

June 11, 2020 - For several years now, banks have been trying to get their customers to move to online banking. If you have been to an older branch bank in the past couple of years, you've probably noticed that there are fewer tellers and more ATMs where the tellers used to be. The reasons for this are simple. Tellers can call in sick and if they work long hours, the law requires the bank to pay them overtime. ATMs will work 24 hours a day, never call in sick and don't make any demands. In short, they are less expensive, easier to work with and more agreeable than live employees.

### Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

The same type of comparison can be made for bank branches. They require a lot of room, are expensive and require the bank to maintain them. If you're a bank and you can push your customers into online banking, you can cut down on your expenses by needing fewer branches and fewer employees. But many bank customers have been slow to adopt these tools. They still want to walk into a branch, talk to a live human being at the teller window and do things the way they have always done them. At least, they did until COVID19.

COVID has had the most profound impact on banking of any single incident. That's because most states implemented restrictions on the way that businesses could operate; including banks. People were told to stay home unless they absolutely needed to go out. And even though bank branches were considered "essential" and remained open, large numbers of consumers migrated to electronic banking very rapidly. And many consumers have found that they not only like this method of banking, but that they intend to keep using it.

In fact, surveys indicate that as many as 40% of consumers who tried electronic banking during COVID19 intend to make it their primary form of banking once the pandemic is over. That's huge, and it is forcing many large banks to retool their business plans. It's also going to force many consumers to make the switch to use electronic banking. That's because their branches are likely to close whether or not they like it.

There is a lot to like about electronic banking for anyone willing to give it a try. You can deposit checks, transfer money, check your balances and pay bills without having to take a single step outside of your home. From a convenience perspective, you really can't beat it. But there are also some significant dangers that it brings.

Hackers are well aware of the move to electronic banking and they are using that move to their advantage. They are rapidly developing malware for smart phones that can steal your banking credentials and drain bank accounts. This isn't theory. It is already happening. Therefore, it is imperative that anyone who uses banking apps also follows some procedures to protect themselves.

Some online banking apps will allow you to store your user name and password in the app. This allows users to log into their account without having to provide a user name or password. While that may be convenient, it isn't wise. Anyone who gets their hands on your unlocked phone or other device will be able to drain your account.

If you are using a banking app on a smart phone, then you should actually make sure that your phone locks automatically when not in use. And you'll want to use a password for this lock, not a fingerprint or a facial scan. In fact, facial scans are probably the worst form of protection you can get. Anyone with a picture of you will have the ability to access your device.

Users should also enable two factor authentication on banking apps when it is available, but they shouldn't rely on it as their only form of protection. That's because two factor authentication normally relies on sending a text message to mobile device to verify that someone logging into an account actually has access to a phone number registered to that account. But you are doing your banking on a smart phone, and the phone number registered to the account is the same as the phone you are using, then two factor isn't going to protect you too well. But it does make it significantly more difficult for anyone to log onto your accounts from another device, so it is worth having.

And finally, anyone using mobile or electronic banking apps needs to be very careful about any other apps they are using on the phone or other devices. It's a fairly easy process for hackers to develop useful apps that also have a nefarious purpose, such as stealing login credentials from banking apps. Malware like this can remain dormant on your computer or phone until you start using a banking app that then triggers the malware to swing into action. Malware can be disguised in any form, include games. To help prevent it, users should install antivirus apps on their smart devices, just as they would on a regular computer.

Although not all bank branches are doomed to close, the way that they operate will change dramatically over the next few years. Branches that remain open are likely to focus on lending and complex transactions, and many of them won't have any tellers at all. So if you haven't tried electronic banking yet, you may want give it a try while you still have some choices and while you can still walk into a local branch and ask questions, just in case you run into any issues.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS