SECURTRUST
FEDERAL CREDIT UNION

The Credit Union Navigator

Volume 20, Issue 3

Credit Union Services

- After-Hours Lending
- ATMs
- Auto Loans
- Automatic Bank Drafts
- BillPay-e PLUS™
- CardValet app
- Certificates of Deposit
- Checking
- Christmas Club
- Credit Life/Disability Insurance
- Direct Deposit
- EFT Service
- GAP Insurance
- IRAs
- Kids Club
- MasterCard Debit Cards
- Mobile Banking
- Mobile Deposit
- Mortgages
- Notary Service
- Online Banking
- Online Loan Applications
- Online Loan Payment
- Payments by Phone
- Personal Loans
- Save-Your-Change
- Savings
- Share Certificates
- Vacation Club
- VISA Credit Cards
- VISA Gift Cards

Martin Luther King Jr. Day

Monday January 18, 2021

Washington's Birthday

Monday February 15, 2021

Memorial Day

Monday May 31, 2021

Branch Information

3870 Goodman Road East
Southaven, MS 38672

Member Services: 662-890-8760
Toll free: 888-419-7723
Business Hours

Monday	8:00 AM – 4:30 PM
Tuesday	8:00 AM – 4:30 PM
Wednesday	8:00 AM – 3:00 PM
Thursday	8:00 AM – 4:30 PM
Friday	8:00 AM— 6:00 PM

Keep control at your fingertips and download CardValet.

CardValet lets you manage card usage through your mobile device by identifying where and how your debitd card(s) can be used.

1. Download the CardValet app.
2. Register your debit card(s)
3. Customize your features.

CardValet

Data rates may apply. Check with your mobile phone carrier for details. CardValet is a registered trademark of Fiserv, Inc. or its affiliates. Copyright 2021 SecurTrust Federal Credit Union. All rights reserved.

Home Banking

Call SecurTrust (662) 890-8760 and ask about home banking — you **can have access to…**

⇒ **Posted Deposits**
⇒ **General Transactions**
⇒ **Transfer money to and from accounts**
⇒ **Check Balances**

Visit WWW.SECURTRUST.ORG or download our SecurTrust APP and take control!

EQUAL HOUSING LENDER

Android Smartphone Malware: How To Tell If Yours Has It And How To Avoid It

Those ugly little viruses that love to live in Android devices are a problem and many users may suspect they have malware but aren't aware of how to tell or what to do about it. Different malware types bring their own symptoms, making it difficult to figure out what type the malware is, much less how to go about removing it. A study in by Malwarebytes found nearly 200,000 circumstances of malware on devices it tested in May and again in June of the previous year. Experts maintain that smartphone malware can be eliminated, and better yet, be avoided to begin with.

Unrelenting ad pop-ups and slow running devices are two types of malware symptoms that can make you want to toss your smartphone off the nearest cliff, but don't! Security experts find the most common are adware apps like *Ads Blocker*, a malware app that does the opposite of what it claims to do. Ads Blocker multiplies the amount of pop-up ads on a device, and every time an ad is clicked someone is making money from it. So, if your device is deluged with ads, and even more so after installing Ads Blocker, you may be in the thick of it.

The second most common malware exploits weakness in smartphones, looking to gain access to PII (personally identifiable information) and other data by giving itself the permission to do so. Once the malware gives itself access to data, user permissions are no longer needed, and users are totally unaware data is being stolen. That data theft also includes putting your contacts in a risky spot, too. Your contacts are now set up for malware infections that include email spear phishing and other socially engineered attacks. Other data up for grabs on an Android device includes financial information, phone numbers and pretty much any other PII currently on the device.

Smartphone Malware Symptoms

- **Your battery is losing juice rapidly**
- **You download an app and the icon immediately vanishes**
- **Constant, unrelenting ad pop-ups no matter what app you're using**
- **Apps you didn't download appear on your device**

Smartphone Malware Prevention

- **Keep a device and apps updated with the latest software versions. They can fix security weaknesses and remove the way the malware entered. They can also prevent malware from working overall.**
- **Delete apps you no longer use and consider investigating and removing an app you suspect may be malware.**
- **Investigate anti-virus software. It can find and alert you to malware on a device, shop around before doing so.**

Only download apps from the official app stores since they routinely scan for infected apps. Getting apps from other sources, called sideloading, is a very risky prospect. Hackers love to load these third-party sites with malware apps, knowing the website does not scan for viruses before making them available.

Remember that malicious actors are sneaky and can make a fake app appear to be legitimate, even if it means just adding a letter to the name or copying a logo. Take the time to check them out, including reading reviews, before downloading anything to your devices.