(Approx. 1201 words)

Modern-Day Bonnie and Clydes Are Trying To Steal Your Identity and Your Money

By Kurt Jefferson, Editor, Central Kentucky Computer Society  
<https://ckcs.org/>

lextown2 \*\* gmail.com

I've written in the past that if Bonnie and Clyde were alive today, they definitely wouldn't waste time robbing banks. If you're not familiar with the couple, they were ruthless gangsters who robbed banks, stores, and other places of business and killed lawmen, shopkeepers, and owners of cars they were stealing in at least four states.

They were, perhaps, best known for robbing more than a dozen banks– some of the same banks twice–over a four-year period, primarily in Missouri, Oklahoma, New Mexico, and Texas. Back in their heyday, they also targeted stores in small towns and funeral homes located in rural areas. Make no mistake about it. They were dangerous lawbreakers. That was how it was in the Depression-era 1930s.

Fast forward to today. Modern Bonnie and Clydes don't rob banks. It's too much work. Instead, they steal personal data from computers, phones, and tablets. They're called hackers. One of their main goals in this life is to steal, rob, and gain access to your hard-earned dollars. Their goal is to grab your money and run; your goal is to keep that from happening. So, whether you're tech-savvy or not, how in the world are you supposed to keep this from happening? There are simple steps you can take.

1. When someone calls you on the phone from an unknown number, DO NOT answer the phone; wait for a voicemail message. Microsoft, Apple, etc., will not call you. These thugs want to get their hands inside your computer or other device to steal your passwords or personal information. If you answer the phone, your number may be sold for more money.

2. Don't open emails from unknown sources. Don't open attachments from unknown senders. Don't respond to schemes alerting you that a friend has been hurt in London, Paris, Sydney, or some other location. Could you send money to help them? Your friend is in the hospital and needs your financial help. Their wallet's been stolen. Their purse has been snatched. And I'm the king of Spain.

Please don't fall for it. Don't click on links in an email from someone you don't usually hear from, urging you to view these great photos. There are no photos. Once you click on the link, malware infects your Windows PC and sends emails to everyone in your address book with the same message, urging them to click on a link to view photos. Phishing is the most successful cybercrime in America.

There were nearly 324,000 victims last year alone. (Phishing refers to an email that appears to be from a legitimate company or organization. There's often a threat – your account will be closed, or the sheriff will come to your house unless you respond. It's all bogus. But plenty of Americans fall for it.) Ever gotten an email that you owe $500 for Norton 360 (virus and malware protection software) that you never even purchased? You'd be surprised by how many folks respond to the email and even pay for the software they don't own. The thugs sending the email are not from Norton. Most junk email trying to get into your wallet originates in Russia, Germany, the U.S., and China.

3. Yes, it's a pain. But what tech folks call two-factor authentication can save your bacon. Turn it on. You'll be blocked if you decide to change your Gmail password, Facebook log-in, iCloud username or password, or some other account, you'll be blocked. You must enter a code you receive in a text message, an email, or even using the Gmail app on your smartphone to get permission to change your password. Yes, as I said, it's a pain. But it's preventing crooks from gaining access to your account. So instead of just changing your passwords, you must first receive a code and enter it into a website or Gmail app. That proves you are who you say you are.

4. Run antivirus software.

For Windows PCs:

Safety Detectives: The Best Windows Antivirus

<https://www.safetydetectives.com/>

PC Mag: The Best Antivirus Software for 2023

<https://www.pcmag.com/picks/the-best-antivirus-protection>

For Macs:

Safety Detectives: Ten Best Antiviruses for Mac in 2023

<https://www.safetydetectives.com/best-antivirus/mac/>

Macworld: Best Mac Antivirus Software 2023

<https://www.macworld.com/article/668850/best-mac-antivirus-software.html>

For Linux:

Safety Detectives: Five Best Antiviruses for Linux in 2023

<https://www.safetydetectives.com/best-antivirus/linux/>

Ubuntu Pit: Top 15 Best Linux Antivirus Programs in 2023

<https://www.ubuntupit.com/best-linux-antivirus-top-reviewed-compared/>

5. Don't go on a fishing expedition on the Web. The World Wide Web is remarkable. It's the best library in the world. There are an estimated 1.6 to 1.9 BILLION websites currently accessible. Less than 400 million are currently active. More than 51% of all people in the world are online. Asia accounts for half the Internet traffic worldwide. Talk about diversity. Websites appear in more than 200 languages. But watch your step. Don't put your foot into horse dung. Make sure the website you visit starts with https. No, this is not always possible.

Some websites refuse to use the "https:" system. The "s" stands for secure. You're accessing a secure website. Don't randomly visit online gambling websites, sites with outdated addresses, websites with shortened addresses, sites ending in .onion, torrent websites (file sharing sites), porn sites and others.

Google constantly scans websites, looking for legitimate websites that have been compromised, unsafe sites, or other questionable pages. If you wonder whether a website is safe or not, visit the web address below and paste your website into Google's Safe Browsing website:

<https://transparencyreport.google.com/safe-browsing/search>

It will tell you whether it's safe to proceed or not.

5. Use a well-regarded virtual private network (VPN).

This tool sends your Internet signal through a tunnel so that hackers and other thieves cannot access the web pages you visit, your email, your passwords, or additional private information. Do your homework. Find a good VPN you can afford.

Steer away from free VPNs because many sell your data online, bombard you with ads, and some even use your computer's processing power.

For Windows PCs:

Privacy Savvy: Five Best VPNs for Privacy

<https://privacysavvy.com/vpn/best/windows/>

VPN Reports: Best of the Best VPNs

<https://www.vpnreports.com/best-vpn/windows/>

For Macs:

VPN Reports: Best VPNs for Mac in 2023

<https://www.vpnreports.com/best-vpn/mac/>

Safety Detectives: Ten Best VPNs For Mac

<https://www.safetydetectives.com/best-vpns/mac/>

For Linux PCs:

Safety Detectives: Five Best Linux VPNs

<https://www.safetydetectives.com/blog/best-linux-vpns/>

Pro Privacy: Ten Best VPNs for Linux

<https://proprivacy.com/vpn/comparison/best-linux-vpn>

6. Use a password manager to track your passwords and log in to many websites requiring a username and password automatically. Experts say this is smarter than allowing your browser to remember your passwords. Unfortunately, web browsers are not really safe to keep that sort of information. As Tom's Guide writes, "That's because desktop web browsers, despite their best efforts, tend to do a lousy job of safeguarding your passwords, credit card numbers, and personal details, such as your name and address. As a result, web browsers are fairly easy to break into, and lots of malware, browser extensions, and even honest software can extract sensitive information from them."

Here are websites where you can read about the best password managers and pick one that works for you:

PC Mag: <https://www.pcmag.com/picks/the-best-password-managers>

Tom's Guide: <https://www.tomsguide.com/us/best-password-managers,review-3785.html>

How To Geek: <https://www.howtogeek.com/780233/best-password-manager/>