COMMON WAYS IDENTITY THEFT CAN HAPPEN:

“OLD FASHIONED” STEALING / DUMPSTER DIVING

Thieves typically steal wallets and purses. They also steal mail such as credit card and bank statements, pre-approved credit card offers, check orders and other financial mail.

Thieves also dig through trash looking for bills, financial or other personal information.

Avoid it by: Shreding all personal documents and credit card offers before throwing them away, and erase / destroy hard drives before you get rid of computers or smartphones.

CHANGE OF ADDRESS SCAM

In recent years, some people have discovered that they had officially moved, even though they hadn't left home at all.

It's called change of address fraud, and it's a growing scam that takes advantage of the Postal Service's mail forwarding system. It's actually a fairly simple act, which is part of the reason why it works so well. Often, all a thief will have to do is fill out a change of address form and drop it off at the nearest post office.

Unlike most fraud attempts, it's actually easier to commit in person than online. Attempting to fraudulently change a person's address online will promptly the Postal Service to seek a small bank withdraw as proof of identity. This, of course, can still be completed by a thief who has already gained access to a victim's banking information – but it's a more complicated process than simply filling out a form with ill-gotten information.

WHAT TO DO…

The good news is that, if you pay attention, you may be able to catch change of address fraud before it goes on for too long. Time Magazine advised readers to simply keep a closer eye on their mailboxes, where signs of address fraud can be quite apparent. You may suddenly stop getting important pieces of mail that you were expecting. You may even receive a notice

informing you of your change of address. If anything seems amiss, contact your local post office immediately.

You should also keep a closer eye on your accounts, in case thieves successfully used your stolen mail to open financial accounts under your name.

PHISHING

Thieves may send unsolicited Emails, pretending to be a financial institution or a company, asking you to click a link to update or confirm your personal or login information. The link is directed to a "spoof" website designed to look like a legitimate site.

Fake emails (phishing) will often…

Ask for personal information. They claim that your information has been compromised and ask you to confirm the authenticity of your transactions.

- Appear to be from a legitimate source. While some emails are easy to identity as fraudulent, others may appear to be from a legitimate address and trusted source. The name or address in the "From" field, can easily be altered.
- Contain fraudulent job offer, such as work-at-home positions.
- Contain prizes or gift certificate offers. In exchange for completing a survey or answering questions, some fake emails promise a prize or gift certificate. They require you to give personal information in order to obtain the prize.
- Links to counterfeit websites. Fake emails may direct you to counterfeit websites that closely resemble a legitimate site while they collect personal information for illegal use.

- Links to real websites. Some fake emails link to legitimate websites. This is done in an attempt to make a fake email appear real.

- Contain fraudulent phone numbers. Never call a number featured on an email you suspect is fraudulent; it can be tied to the fraudsters.

- Contain real phone numbers. Similar to linking to real websites, real phone numbers may be featured in a fake email in an effort to make the email appear legitimate.

WHAT TO DO…

If you receive an e-mail that looks like it is from Citizens Bank of Kentucky or another well-known company requesting financial information or any other personal or sensitive data, please take the following actions:

- Treat the e-mail with suspicion.
- Do not reply to the e-mail or respond by clicking on a link within the e-mail message.
- Do not download anything or open attachments.
- Report the suspicious e-mail to the FTC and forward the e-mail to **uce@ftc.gov**.

If you have already provided personal financial information via e-mail and feel your Citizens Bank of Kentucky accounts are in jeopardy, contact our bank as soon as possible to report the suspicious activity. You can reach an Account Information Center representative by calling 1-866-462-2265 (Bank) or via email: **info@wercitizens.bank**.

SKIMMING

Thieves may use a card reader device to copy the card’s magnetic strip to duplicate without the card owner’s knowledge.

WHAT TO DO…

Check for Tampering

When you approach an ATM, check for some obvious signs of tampering at the top of the ATM, near the speakers, the side of the screen, the card reader itself, and the keyboard. If something looks different, such as a different color or material, graphics that aren't aligned correctly, or anything else that doesn't look right, don't use that ATM. The same is true for credit card readers.

Wiggle Everything

Even if you can't see any visual differences, push at everything, Tanase said. ATMs are solidly constructed and generally don't have any jiggling or loose parts. Credit card readers have more variation, but still: Pull at protruding parts like the card reader. See if the keyboard is securely attached and just one piece. Does anything move when you push at it?

Counterfeit websites (SPOOFING)

Online thieves often direct you to fraudulent websites via email and pop-up windows in an attempt to collect your personal information. In many cases there is no easy way to determine that you are on a phony website because the URL will contain the name of the institution-this is spoofing. If you type or copy/paste the URL into a new browser window and it does not take you to a legitimate website, or you get an error message, it was probably just a cover for the fake site.

WHAT TO DO…

When logging into your account, look closely at your browser. The address in the location bar should start with "https"-for example, https://www.wercitizens.bank. You should also see a lock icon at the bottom of the browser. If you double-click the icon, it should display security information about Citizens Bank of Kentucky.

PROTECTING YOURSELF ONLINE

As your financial institution, we work hard to protect you from fraud. But you and your computer are the front line of defense. In just a few simple steps, you can help keep your computer-and your finances-safe.

- *Secure your passwords*

A good password should:

- Not be based on personal information that can be easily guessed (your pet's name, birth date, etc.)
- Not be a word that can be found in any dictionary of any language.
- Contain 8 characters, at least 1 number, at least 1 uppercase letter, at least 1 lowercase letter, and password cannot contain leading or trailing blanks.
- Not be the same as any password you use for anything else.
- Always memorize your password and do not write it down. Citizens Bank of Kentucky will prompt changing your passwords every 90 days.

Citizens Bank of Kentucky will not ask for your online banking ID or password by telephone OR by email!

- *Secure your computer*

There are certain precautions you should take to keep your computer safe from viruses and hackers.

- Keep your operating system and browser up to date.
- Use up-to-date anti-virus and anti-spyware software – and set them to update automatically.
- Use a personal firewall.
- Activate a pop-up blocker.

Keep in mind:

Security software that comes pre-installed on your computer typically works for just a few months unless you pay to extend its usage. Avoid buying software in response to unexpected pop-up messages or ads that claim to have scanned your computer and detected malware. That can be a scare tactic scammers use to spread malware.