ACCESSbank®

# Digital Banking Safety: Tips for Youth Bankers & Parents

**Teens and Tweens can face unique risks specifically targeting them with scams promising quick cash for cashing checks, false online shopping deals, identity theft and social media connections with fraudulent intentions. Parents should open the lines of communication early and often.**

## Scammers tend to target youth bankers in their favorite habitat—the Internet.

- Fraudsters use social media to trick teens into providing personal information, which can be used for identity theft.
- Many scams take the form of ads and online offers, promising luxury goods for amazingly cheap prices — goods that never arrive.
- Other scams involve contests, scholarships, or employment opportunities that require the teen to pay some sort of fee or deposit.
- Yet another trick is to lure teens with free services for smartphones that incur a monthly charge.

## Major Scams affecting Youth Bankers

**Social Media scam:** Among scams common to social media are those involving identity theft such as surveys or contests that request personal information and catfishing in which the scammer poses as someone they are not and befriends the victim with the intention of taking money, personal information, or more.

**Online Shopping scam:** Often lured into phony websites that take their money and sell them nothing or providing personal information used for purposes of identity theft or tricked into clicking on links and downloading malware. Finding the latest iPhone, designer handbag, or state-of-the-art headphones for a fraction of the retail price sounds too good to be true. Unfortunately, that's exactly what it is: too good to be true. They purchase items that never arrive.

**Talent and Modeling scams:** Acting and modeling scams can be found all over the Internet. But more recent scams involve skill-based contests in which teens are urged to enter artwork, music compositions, or creative writing in order to win money or fame. These scams might require an entry fee and if the teen wins, more cash. Spoiler alert: The entry wins, and teens are hit up with an additional fee or fees supposedly to help with the cost of promotion, publication, and so forth.

**Online Auction scams:** These target unsuspecting teens in various ways. One scam involves an auction that the teen wins for an item that doesn't exist or never arrives—even after the teen paid for the item. Alternatively, teens are encouraged to auction off possessions, the scam artist (the auction house rep) requires the teen to send in the item in advance, before the buyer's payment arrives, or even before bids are placed. Of course, the funds never arrive, the auction never happens, and the scammer disappears.

# Digital Banking Safety: Tips for Youth Bankers & Parents

## Follow these tips to avoid scams

1. Log out of your online banking or mobile banking app session after you're finished.
2. Be careful when using your phone or computer in public – assume someone could be watching. Never leave your device unattended.
3. Keep your devices updated to the latest versions of software and anti-virus protection.
4. Change passwords every 2-3 months and choose strong passwords. Mix numbers, characters, upper and lower case. Do not use common words or dates.
5. Never share your password or account information with anyone, even a friend.
6. Make sure to set up transaction alerts. If you get an alert for a transaction that you did not make, immediately contact customer service.
7. Never access your banking account through hyperlinks in emails, pop-up ads, or search engines. Go directly to your online banking URL or use the official banking app.
8. When purchasing something online, learn to spot fake websites. Look for spelling errors, fake logos, strange images, incomplete web addresses.
9. Never send money to anyone that you do not personally know and trust on the internet or from your phone.
10. Avoid using public computers and public Wi-Fi when accessing your bank account.