

# Protect Your Business from Online Fraud

We want to make you aware of a growing type of online fraud that is impacting businesses worldwide. Increasingly, criminals are stealing valid Internet Banking credentials belonging to small and medium-sized businesses to transfer funds fraudulently.

## THE THREAT

Sophisticated identity thieves are targeting business computers to access confidential and sensitive information. Once these criminals tap into your computer system, they can acquire your Login IDs and Passwords and pose as you to access your online accounts, including your bank accounts.

This identity theft technique does not involve a breach of bank security — instead, it is typically carried out via a “spear phishing” email that directly names the recipient and contains either an infected file or a link to an infectious website. Once the user opens the attachment, or clicks the link to open the website, malware is covertly installed on the user’s computer that usually consists of a keystroke logger, which logs the user’s credentials and sends it to the criminals.

## INTERNET BANKING IMPACT

This type of fraud allows criminals to transfer funds electronically from a deposit account using wire transfer, Bill Pay, or Automated Clearinghouse (ACH). Funds withdrawn from the account are typically routed to banks in the U.S. and credited to the identity thieves’ accounts. The funds are then promptly withdrawn or wired overseas, making recovery extremely difficult.

It is important for you to understand and remember that, according to our Internet Banking Access Agreement, we consider a transaction to be authorized by you and will honor online instructions we receive when the proper Login ID and Password are given. We will not be liable for losses if your Login ID and Password are stolen through an unprotected computer, except where required by law.

At Landmark Bank, we do all we can to ensure your transactions are secure. However, there are some measures only you can take to protect your business. Take time to implement the safe Internet Banking practices listed here at your business.

Additional information is available on our website at [www.landmarkbank.com/protectyourself](http://www.landmarkbank.com/protectyourself).



Member FDIC

## TIPS FOR SAFER INTERNET BANKING

### Protect your Passwords and Login ID

Do not let employees share Login IDs, Passwords, or other individual security measures.

### Require strong Passwords

The strongest Passwords will contain a combination of upper and lower case letters, numbers and characters such as !@#%&\* and are at least 10 characters long. Change Passwords every 60 days.

### Always sign off

Always log off from your Internet Banking session by using the “Exit” button.

### Protect computers with anti-virus and firewalls

Talk to your computer security expert to determine the best protection for your system. Determine how often your software and security measures should be updated.

### Designate a computer for online banking

Limit the use of the computer that you use for online banking. You are less likely to get a virus or harmful program/software downloaded to your computer if you don’t allow any other online activity on that computer, including email.

### Only use company wireless Internet and computers

Do not allow employees to access Internet Banking from public computers or public wireless Internet such as coffee shops, library, book stores, etc.

### Dual authorization

Setup dual authorization controls for all ACH and wire transfer payments with a separate originator and authorizer through Landmark Bank’s Internet Banking.

### Reconcile bank account daily

Due to limitations on returning unauthorized transactions on business accounts, it is important to reconcile your bank account daily. This enables you to identify unauthorized transactions and start proceedings for reversing the transaction.

### Do not email sensitive information

Email is not generally encrypted and communications sent via email should be considered high risk. Communication of sensitive information should be done in person or over the phone after positive identification is made. Landmark Bank will never send, or ask you to send, sensitive information via email. If you need to send a document with confidential information, consider sending it encrypted or by fax.