OLD DOMINION
NATIONAL BANK

# INFORMATION SECURITY

*Welcome to Old Dominion's Information Security overview. Your privacy and the security of your confidential information is important to us. Here are some tips and tools to help us protect you.*

## Phishing

If you open an email or text requesting confidential information such as social security number or account numbers be wary and validate the sender and confirm the legitimacy of the request.

An example of a phishing message is "*We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*

Old Dominion National Bank will not send these types of messages. If you receive one presenting itself as being from us do not respond and contact us immediately.

## Hacked Email

You may have been hacked if:

- friends and family are getting emails or messages you didn't send
- your Sent messages folder has messages you didn't send, or it has been emptied
- your social media accounts have posts you didn't make
- you can't log into your email or social media account

If you believe you may have been hacked:

1. Update your system and delete any malware: Make sure your security software is up-to-date

2. Change your passwords: That's IF you're able to log into your email or social networking account. Someone may have gotten your old password

and changed it. If you use similar passwords for other accounts, change them, too. Make sure you **create strong passwords** that will be hard to guess.

3. Check the advice your email provider or social networking site has about restoring your account. You can find helpful advice **specific to the service**. If your account has been taken over, you might need to fill out forms to prove it's really you trying to get back into your account.

4. Check your account settings: Once you're back in your account, make sure your signature and "away" message don't contain unfamiliar links, and that messages aren't being forwarded to someone else's address. On your social networking service, look for changes to the account since you last logged in — say, a new "friend."

5. Tell your friends & your bank: A quick email letting your friends and bank know they might have gotten a malicious link or a fake plea for help can keep them from sending money they won't get back or installing malware on their computers. Put your friends' email addresses in the Bcc line to keep them confidential. You could copy and send this article, too.

### Identity Theft

If you believe your information has been compromised take immediate action to limit what the thief can do:

1. Place an initial fraud alert on your credit report
2. Order your credit reports to review all details for accuracy
3. Create an Identity Theft Report

The Federal Trade Commission provides valuable resource to walk you through repairing identity theft. Visit them online at:

http://www.consumer.ftc.gov/articles/0274-immediate-steps-repair-identity-theft