FRAUD & RISK *Awareness*

PROTECTING YOUR DEBIT CARD

- When purchasing something in a store, it's safest to use your mobile wallet. Otherwise, use Tap to Pay (contactless). Chip transactions are okay, but avoid swiping your card when possible. For purchases online, your mobile wallet is always your best bet.

- Within the Manage Cards option of digital banking, you can activate your card and set your PIN. But did you know that you can also add travel notifications and use Card On/Card Off to protect your card anywhere, anytime?

- Sign up for our free card alerts via text or email any time your card is used, whether the transaction is approved or denied. See something you didn't authorize? Turn your card off in Card On/Card Off within your digital banking, then call us for further assistance.

- Our card alerts are informative - they don't prompt you to reply or call a phone number provided within the text. They do not push you with urgency and don't include a link to use to log in. They only reference card activity - they won't notify you of an account closure or freeze any other type of activity. Our alerts come from the short number 662265 and are in the following simple format: *Legence Bank: Approved debit purchase with card *1234 for $100.00 at Target*

- Be wary of making purchases from sketchy websites and apps - they might exist primarily to steal and sell or use your card info.

- Don't let anyone borrow your card - they could save the info before giving it back and make purchases online or tie it to their CashApp, Venmo, PayPal, etc.

- If someone calls you and asks you for your full card number, expiration date, and/or CVV on the back of your card, it's a scam. If someone calls you and tries to prove they're your banker by providing you with the first 8 digits of your card number, that is public information, and that is a scam. They're imposters trying to build a fake trust.

PROTECTING YOUR DIGITAL BANKING

- Never share your digital banking username and password with anyone. Create strong passwords that are unique - don't use the same password across multiple websites.

- Never share the one time passcodes (security codes) that are sent to you as part of your digital banking login. They're automatically generated by digital banking upon login. No one, no matter how official or legitimate they sound on the phone, should ever ask you for that code. We do not use one time passcodes to verify you.

- Be wary of providing your banking credentials with any third party, even if it's to apply for a loan, buy cryptocurrency, or set up budgeting software with a seemingly legitimate company. Though it provides convenience, it can expose you to serious privacy and security risks.

- Keep your devices and software up to date - this is essential for security. Updates often patch vulnerabilities and fix known bugs. Within the settings of your devices, you most likely have an option to automatically download and install updates as they become available, making this process easy.

- Enroll in digital banking alerts within the Manage Alerts option in the menu. Your many options include failed login alerts, password or email change alerts, balance alerts, and bill pay and transfer alerts. Knowledge is power!

- Did you receive a text or call about unauthorized activity, and the caller told you they need remote access to your device to get your money back? Did they ask you to log in to your digital banking while they had remote access, or maybe even ask you for your credentials and security codes? That's a scam.

- We will never ask you to move your money in order to protect it. We won't ask you to send a P2P transaction through SPIN (or other payment apps like CashApp, Venmo, or PayPal). We won't ask you to buy bitcoin, purchase gift cards, send a cashier's check or wire, or withdraw cash and put it in a bitcoin ATM to protect your money. Ever.

PROTECTING YOURSELF

- Trust your intuition. If something feels off, it usually is. Step back and look at the situation - does it make sense? Ask someone who you trust what they think.
- Don't reply to suspicious emails or texts. Pause before you click on a link or a pop-up, and slow down before opening attachments from people you don't know.
- Don't trust caller ID - it's really easy to spoof that now. If unsure, hang up, research the true phone number for the company and call them back using that phone number.
- Fraudsters often create a false emergency or opportunity that requires immediate action. They may claim your account is at risk, a loved one needs help, or an investment window is closing. The goal is to make you act before you have time to think or verify the story. Healthy relationships - personal or professional - do NOT require secrecy or financial control. We encourage you to slow things down and speak with someone you trust first.
- Be on alert for any of the following red flags:
  - Someone is pressuring you to move your money quickly. They tell you that you can't trust the bank, so you should lie about the reason for your transaction or keep it all a secret. They may insist on staying on the phone with you during purchases in a store or transactions in a bank.
  - Someone opens an account in your name without your involvement. They may send you checks with your name on them or ask you to send money to your new account. But you never signed a signature card or had anything to do with it.
  - Someone tells you that you have to move almost all of your money to "protect it" or for the purposes of "asset verification".
  - Someone you talk to online but have never met in person asks you for financial help. They insist they're coming to meet you in person soon, but an emergency popped up and they need your help today.
  - Someone asks you to send or receive money on their behalf, or they ask for access to your finances.
  - During the sale of an item in an online marketplace, someone either overpays you for something you're selling and wants you to return the difference, or they demand payment on something you're purchasing before you ever see it.
  - Someone told you that you've won a prize or a sweepstakes, but that you have to pay to claim your winnings.
  - Someone hired you for a new online job, but you have to pay to start working there, or your first task involves moving money.
  - Someone prompts you to use a bitcoin ATM in any capacity.
  - Someone asks you to buy gift cards as a form of payment or a way to protect your money.
  - Someone claims you or a loved one is in trouble and the only thing that can fix it is money - now.
  - Financial pressure from family and friends can be a warning sign - never let yourself feel rushed or obligated when it comes to your money.
- Do you have any questions or concerns regarding fraud? Please reach out to Legence Bank's Risk Prevention & Intelligence Department - we'd love to help you gain peace of mind!

FRAUD & RISK *Awareness*

PROTECTING YOUR DEBIT CARD

- When purchasing something in a store, it's safest to use your mobile wallet. Otherwise, use Tap to Pay (contactless). Chip transactions are okay, but avoid swiping your card when possible. For purchases online, your mobile wallet is always your best bet.

- Within the Manage Cards option of digital banking, you can activate your card and set your PIN. But did you know that you can also add travel notifications and use Card On/Card Off to protect your card anywhere, anytime?

- Sign up for our free card alerts to receive a text or email any time your card is used, whether the transaction is approved or denied. See something you didn't authorize? Turn your card off in Card On/Card Off within your digital banking, then call us for further assistance.

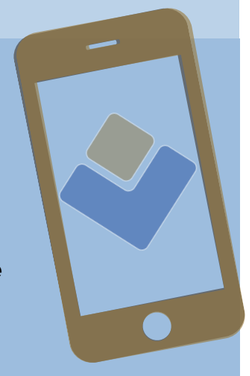
- Our card alerts are informative - they don't prompt you to reply or call a phone number provided within the text. They don't push you with urgency and don't include a link to use to log in. They only reference card activity - they won't notify you of an account closure or freeze any other type of activity. Our alerts come from the short number 662265 and are in the following simple format: *Legence Bank: Approved debit purchase with card *1234 for $100.00 at Target*

- Be wary of making purchases from sketchy websites and apps - they might exist primarily to steal and then sell or use your card info.

- Don't let anyone borrow your card - they could save the info before giving it back and make purchases online or tie it to their CashApp, Venmo, PayPal, etc.

- If someone calls you and asks you for your full card number, expiration date, and/or CVV on the back of your card, it's a scam. If someone calls you and tries to prove they're your banker by providing you with the first 8 digits of your card number, that is public information, and that is a scam. They're imposters trying to build a fake trust.

PROTECTING YOUR DIGITAL BANKING



- Never share your digital banking username and password with anyone. Create strong passwords that are unique - don't use the same password across multiple websites.

- Never share the one time passcodes (security codes) that are sent to you as part of your digital banking login. They're automatically generated by digital banking upon login. No one, no matter how official or legitimate they sound on the phone, should ever ask you for that code. We do not use one time passcodes to verify you.

- Be wary of providing your banking credentials with any third party, even if it's to apply for a loan, buy cryptocurrency, or set up budgeting software with a seemingly legitimate company. Though it provides convenience, it can expose you to serious privacy and security risks.

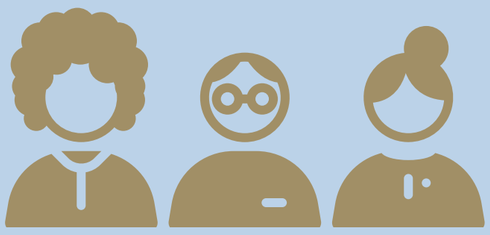
- Keep your devices and software up to date - this is essential for security. Updates often patch vulnerabilities and fix known bugs. Within the settings of your devices, you most likely have an option to automatically download and install updates as they become available, making this process easy.

- Enroll in digital banking alerts within the Manage Alerts option in the menu. Your many options include failed login alerts, password or email change alerts, balance alerts, and bill pay and transfer alerts. Knowledge is power!

- Did you receive a text or call about unauthorized activity, and the caller told you they need remote access to your device so that you can get your money back? Did they ask you to log in to your digital banking while they had remote access, or maybe even ask you for your credentials and security codes? That's a scam.

- We will never ask you to move your money in order to protect it. We won't ask you to send a P2P transaction through SPIN (or other payment apps like CashApp, Venmo, or PayPal). We won't ask you to buy bitcoin, purchase gift cards, send a cashier's check or wire, or withdraw cash and put it in a bitcoin ATM to protect your money. Ever.

FRAUD & RISK *Awareness*



PROTECTING YOURSELF

- Trust your intuition. If something feels off, it usually is. Step back and look at the situation - does it make sense? Ask someone you trust what they think.

- Don't reply to suspicious emails or texts. Pause before you click on a link or a pop-up, and slow down before opening attachments from people you don't know.

- Don't trust caller ID - it's really easy to spoof that now. If unsure, hang up, research the true phone number for the company and call them back using that phone number.

- Fraudsters often create a false emergency or opportunity that requires immediate action. They may claim your account is at risk, a loved one needs help, or an investment window is closing. The goal is to make you act before you have time to think or verify the story. Healthy relationships - personal or professional - do NOT require secrecy or financial control. We encourage you to slow things down and speak with someone you trust first.

- Be on alert for any of the following red flags:
  - Someone is pressuring you to move your money quickly. They tell you that you can't trust the bank, so you should lie about the reason for your transaction or keep it all a secret. They may insist on staying on the phone with you during purchases in a store or transactions in a bank.
  - Someone opens an account in your name without your involvement. They may send you checks with your name on them or ask you to send money to your new account. But you never signed a signature card or had anything to do with the process.
  - Someone tells you that you have to move almost all of your money to "protect it" or for the purposes of "asset verification".
  - Someone you talk to online but have never met in person asks you for financial help. They insist they're coming to meet you in person soon, but an emergency popped up and they need your help today.
  - Someone asks you to send or receive money on their behalf, or they ask for access to your finances.
  - During the sale of an item in an online marketplace, someone either overpays you for something you're selling and wants you to return the difference, or they demand payment on something you're purchasing before you ever see it.
  - Someone told you that you've won a prize or a sweepstakes, but that you have to pay to claim your winnings.
  - Someone hired you for a new online job, but you have to spend your own money to start working there, or your first task involves moving money.
  - Someone prompts you to use a bitcoin ATM in any capacity.
  - Someone asks you to buy gift cards as a form of payment or a way to protect your money.
  - Someone claims you or a loved one is in trouble and the only thing that can fix it is money - now.
  - Financial pressure from family and friends can be a warning sign - never let yourself feel rushed or obligated when it comes to your money.

CONTACT:

RISK PREVENTION & INTELLIGENCE DEPT

(800)360-8044

FRAUD@LEGENCEBANK.COM

Legence® Bank Member FDIC