COVID-19 UPDATE

HOW YOU CAN PROTECT YOUR INFORMATION

CYBERSECURITY BEST PRACTICES

We consider your account security as a partnership between you and BOK Financial®. Following these best practices can go a long way toward keeping you and your personal information more secure, helping protect you from identify theft, and maintaining more secure accounts.

Be Strategic With Your Login Credentials and Passwords

- **Create A Unique Username**
  Do not use personal information such as your social security number or birthday as part of your username.

- **Use Strong Passwords**
  Make sure you use strong, unique passwords for each financial institution you do business with and change it regularly. Consider using a password manager to create, manage, and store passwords that are unique and secure.

- **Do Not Reuse Passwords**
  Never reuse passwords for multiple online accounts. Cyber criminals will try to use passwords they obtain to access other online accounts.

- **Add Tough Security Questions**
  We may prompt you to answer one of your security questions when you log in from a new computer for the first time or change your password.

  Don't share security questions with anyone. Make your answers easy enough for you to remember, but hard for anyone else to guess.

- **Do Not Share Your Password**
  We will never ask you for your password. If you receive an email asking for your login credentials, do not respond as it is not from an authorized BOK Financial representative. Our representatives never have knowledge of your encrypted password. In addition, don't share your password with anyone, including family members.

- **When You Should Change Your Password**
  You should immediately change your password if you:
  - Use the same password for multiple online accounts
  - Believe your password has been stolen
  - Shared your password with someone
  - Provided your password in a phishing email

Monitor Your Accounts

- **Monitor Your Account**
  It's important to access your account frequently to look for changes that you didn't initiate. If you notice something is different, contact us immediately.

- **Review Your Account Statements**
  It's also important to review your account statements regularly for suspicious activity.

- **Check Your Contact Information**
  Check your phone number, address, and email regularly to make sure it's up-to-date so we can contact you quickly, if necessary.

- **Switch To Online Statements**
  We encourage you to switch to online statements to protect sensitive information from getting lost or stolen. If you receive paper statements, shred them before disposing of them.

- **Pay Attention To Email Notifications**
  Email notifications from BOK Financial contain important information about recently initiated transactions and changes made on your account. If you didn't request the transaction or change, please contact us immediately.

Keep Your Technology Up To Date

- **Keep Your Equipment Updated**
  Keep your web browser and operating system up to date, and be sure you're using appropriate security settings. Old software, operating systems, and browsers can be susceptible to attack.

Be Aware Of Phishing Scams

- **Look Out For Phishing Emails**
  Look out for suspicious emails and protect yourself from phishing attempts and malicious links. Don't open links or attachments to emails you're not expecting, even if they look legitimate.

Be Sure You're On A Secure Website

- **"S" Stands For Secure**
  Secure sites begin with "https://" instead of "http://". That means the site is encrypted and minimizes the chances of your information being intercepted as it travels from your computer to the website's server.

- **Look Out For Spoof Websites**
  Cyber criminals use imposter websites to trick you into giving them your information. They can set up a website that looks similar to the one you use and trust, with a few differences. Look for misspellings, grammar changes, and odd imagery. Never go to a website by clicking a link in an email. Always type the URL manually in your browser. On our website, look for the padlock icon in the address bar to confirm that you're on our official, secure site.

- **Download Software And Apps Carefully**
  Downloading programs or games to your computer from the internet can be risky. Don't download anything unless you're confident of the provider. Do a little research first if you're unsure of the provider's safety. Download apps only from the Google Play™ Store or the Apple App Store®.

- **The Importance of Logging Out**
  Online fraud can happen when you move from one website to another without logging out. Make sure to always log out of your online account before you close the window.

Take Precautions At Home

- **Safeguard Your Mobile Devices**
  Using a PIN or lock function is the simplest and most important thing you can do to improve security on your mobile devices—especially if it's lost or stolen. Some devices also use biometrics, like facial recognition or a fingerprint. Use these security enhancements if you have them.

- **Protect Your Home Computer**
  Install anti-virus and anti-spyware software on all computers and mobile devices.

- **Secure Your Home Wi-Fi**
  Secure your network by adding a unique password, only give it out to people you trust, and consider changing the password from time to time.

STEPS TO TAKE IF YOU HAVE A SECURITY ISSUE

Report The Issue
If you suspect fraud or identity theft with your account or to report a security issue, contact us immediately.

Keep An Eye On Account Activity
Check your online account activity regularly over the next few weeks for unexpected transactions, contact us immediately if you suspect unauthorized activity.

Update Your Antivirus Software
Run an antivirus scan to ensure that your computer is not infected with a virus. Make sure that your system and anti-virus software are up-to-date.

Change All Your Passwords
Change your password and security questions immediately for your BOK Financial account, your email account, and other online accounts.

Request A Fraud Alert Be Put On Your File
Contact one of the three major credit bureaus to place a fraud alert on your file so that financial institutions and credit card companies will be required to contact you before opening any new accounts in your name.
- TransUnion: 800.680.7289
- Equifax: 800.525.6285
- Experian: 888.397.3742

File A Report With The Federal Trade Commission (FTC)
The FTC conducts investigations based on consumer complaints to better help with identity theft and online fraud issues.

Learn More
Visit these sites for more information and best practices:

StaySafeOnline.org
Review the STOP. THINK. CONNECT.™ cybersecurity educational campaign.

OnGuardOnline.gov
Tips to help you stay safe and secure online.

https://www.fbi.gov/scams-and-safety
FBI Scams and Safety

BOK FINANCIAL