Online Banking Security Tips

Passwords

MAKE IT UNIQUE
Create a unique password for each website you use. If you do not, one breach leaves all your accounts vulnerable.

MAKE IT COMPLEX
The longer the password, the tougher it is to crack. Use a password with at least 14 characters. Avoid using obvious passwords, like names, dat4es, or standalone dictionary words.

DO NOT SHARE
Never share your password over the phone, in text, by email, or in person. If you are asked for your password, it is probably a scam.

USE A PASSWORD VAULT
Choose passwords you can remember without writing it down. If you cannot remember all your passwords, consider using a password vault.

Mobile Device Security

AUTHENTICATE
Require a passcode and/or biometrics to access your device.

INSTALL UPDATES
Install patches and updates as soon as possible once they become available.

SIGN OUT
"Sign Out" or "Log Off" when finished with an app, rather than just closing it.

LOCK THE SCREEN
When your device is not in use, lock the screen to prevent unauthorized access to it.

SECURE THE DEVICE
Enable security features (e.g., auto-wipe, auto-lock, biometrics, etc.). Install anti-malware, when possible. Do not jailbreak or otherwise circumvent security controls on your device.

DISPOSE CAREFULLY
Before disposing of your mobile device or when changing ownership, delete all information from the device. Use a "factory reset" to permanently erase all content and settings stored on the device.

Online Security

SUSPICIOUS LINKS
Never click suspicious links in emails, on social media posts, or via online advertising. Links can take you to a different website than the labels indicate.

WHEN IN DOUBT,
DO NOT CLICK.

ENCRYPT DATA
Protect your data by only submitting sensitive information to websites that encrypt your data Make sure the URL begins with https:// instead of just http://. (The "s" means your data will be encrypted when you submit it.) Some browsers also display a closed padlock.

PUBLIC TECHNOLOGY
Avoid using public computers or public wireless access points for online banking and other activities involving sensitive information, when possible.

BE CAUTIOUS
Always be cautious if you receive an unsolicited phone call, text, or email directing you to a website or requesting sensitive information.

Computer Security

WATCH FOR MALWARE
Maintain active and up-to-date anti-malware protection provided by a reputable vendor. Schedule regular scans of your computer, alongside real-time scanning, when possible.

If you suspect your computer is infected with malware, discontinue using it for banking, shopping, or other activities involving sensitive information and/or seek professional help to find and remove the malware.

UPDATE SOFTWARE
Update your computer software frequently to ensure you have the latest security patches. This includes your computer's operating system, as well as other installed software (e.g., web browsers, Adobe programs, Microsoft Office, etc.). Automate software updates, when possible, to ensure it is not overlooked.

PHYSICAL SECURITY
Keep your computer in a secure location. Do not leave laptops unattended in untrusted locations (e.g., car, restaurant, airport, etc.).

Learn More

To learn more about securing your online banking activities, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov

Using Strong Authentication

About Authentication

Authentication is the process of verifying a user is who they are before granting the user access to request resources.

There are multiple ways to verify someone is who they claim to be. These are most often split into three categories.

SOMETHING YOU KNOW
This could be a password, pin, social security number, etc.

SOMETHING YOU HAVE
This could be generated by a token, an authenticator mobile app, a text message or phone call sent to your mobile device, etc.

SOMETHING YOU ARE
This is commonly referred to as "biometrics" and could be achieved through fingerprint reader, facial recognition, iris scanner, etc.

Single-Factor

Single-factor authentication occurs when you would only need to provide one method of verification.

The most common form of single-factor authentication happens when someone would provide only a username and password to sign into an account.

In this scenario, the user would only need to know the password to gain access. This is inherently insecure because if the password get compromised, the while account can get compromised.

If single-factor authentication is used, a compromised password can lead to issues such as:

- Loss of Money
- Installation of Malware
- Data Theft or Destruction
- Loss of Reputation

BOTTOM LINE
Single-factor authentication is not considered secure enough to protect your most valuable assets.

Multi-Factor

Multi-factor authentication (MFA) is considered a much stronger and more secure authentication option.

MFA occurs when you require more than one form of authentication to access a system.

For example, instead of just providing a username and password, you would also need to enter a code you receive on your phone.

This is helpful because it means that even if your password gets compromised, an attacker would still need to have physical access to your mobile device to get into your account.

BOTTOM LINE
Enable MFA wherever you can, but especially on your high-risk accounts like internet banking, payment apps, email, online shopping, and social media.

Learn More

To learn more about cybersecurity awareness and using strong authentication, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov

Mobile
Financial Services

Mobile Device Protection

PASSCODES

Create a complex passcode for your mobile devices. Avoid using personal information (e.g., names, dates, etc.) in your passcodes. Do not share your passcodes with anyone.

SECURITY FEATURES

Enable available security features, such as biometrics (e.g., fingerprint scanner, facial recognition, etc.), auto-wipe after number of failed passcode attempts, and auto-lock after a certain amount of time.

UPDATES

Keep your device up to date. Install new updates as soon as you can to fix any identified security vulnerabilities.

AVOID COMPROMISE

Do not root, jailbreak, or otherwise circumvent security controls on your device. Install anti-malware, when possible.

SCREEN LOCK

Lock your device's screen anytime you are not using it, so it must require authentication before the device can be used again.

Mobile Applications

Download and install mobile apps only from trusted sources authorized by the device manufacturer, such as the App Store, Google Play Store, or Microsoft Store.

When possible, require authentication to download mobile apps to prevent unauthorized installation.

Protect yourself from fraudulent mobile apps by watching for these guys.

- Typos
- Poor image quality
- Formatting issues
- Low download number
- Negative user reviews

Review other mobile apps created by the app developer to validate the application's legitimacy.

If possible, create4 a passcode on mobile applications which can access your personal information (e.g., mobile banking services).

When finished with a mobile app, always "Sign Out" or "Log Off" rather than just closing it.

Be On Alert

People are trying to steal your personal information. Remember to be on alert for the following types of threat to your mobile financial services.

SOCIAL ENGINEERING

Phishing is a social engineering tactic used to obtain personal information by masquerading as a trustworthy person via electronic communications (e.g., email, text messages, phone call. etc.).

UNSECURED NETWORKS

If you can connect your phone to a wifi network without entering a password, unauthorized individuals can, too. If you are on an unsecured wireless network, such as a mobile or wifi hotspot, do not use your mobile device to transmit sensitive data.

COMPROMISED WEBSITES

Watch for potentially compromised websites. If th website has a security error or your browser gives you a warning about the site, use caution. If you go to one web address and are redirected to another, close your mobile device's browser immediately and remember:

When in doubt, do not click.

Learn More

To learn more about securing your mobile financial services, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov

Avoiding Social Engineering Attacks

Social Engineering

In a social engineering attack, an attacker tries to manipulate a person into performing an action or disclosing information.

People have a natural tendency to trust. Social engineering attacks exploit this tendency in order to steal your data.

Once the attacker gets your information, they can use it to commit fraud or steal your identity.

Criminals use a variety of social engineering attacks to steal information, including website spoofing and phishing.

This brochure explains the meaning of these common attacks and provides tips you can use to avoid becoming a victim.

Website Spoofing

Website spoofing is the act of creating a fake website to mislead people into sharing sensitive information. Spoofed websites are typically created to look exactly like a legitimate website published by a trusted organization.

PREVENTION TIPS

Pay attention to the web address (URL). A website may look legitimate, but the URL may be misspelled or different.

Do not click links on social media sites, pop-up windows, or non-trusted websites. Typing an address into your browser is a safer alternative.

Avoid using websites if your browser displays certificate errors or warnings.

Only type sensitive information (e.g., credit card numbers, social security numbers, etc.) into websites you have verified are legitimate. Make sure the URL begins with https:// instead of just http://. (The "s" means your data will be encrypted when you submit it.)

If you are suspicious of a website, close it and contact the company directly.

Phishing

Phishing happens when an attacker attempts to acquire information by masquerading as a trustworthy entity via email, text message (smishing), or phone call (vishing).

PREVENTION TIPS

Delete email, text, and social media messages which ask you to share sensitive information. Legitimate companies will not ask you for information this way.

Do not click links or open attachments in unexpected messages or from unknown senders.

If someone contacts you, but it seems suspicious, try to verify if it is legitimate in another way.

For example:

- Navigate to the website yourself.
- Call the sender to verify
- Perform a web search

When in doubt, do not click.

Contact Us

Contact us if you suspect you have fallen victim to a social engineering attack and have discolored information related to your account(s).

Regularly monitoring your account actively or enabling transaction alerts is a good way to detect fraudulent activity.

If you notice unauthorized account activity, notify us immediately.

HOW TO REPORT

If you need to report suspicious activity, please contact:

Heritage Bank
ORGANIZATION

support@ourhbna.com
EMAIL ADDRESS

www.ourhbna.com
WEBSITE

Learn More

To learn more about avoiding social engineering attacks, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov