Online Security

Visit our Online Education Center on our website under the **About Us** tab to view additional information on Online Security.

Recommended Financial and Information Security Practices

At Village Bank, we ensure your confidential information is being protected. We maintain physical, electronic, and procedural safeguards that comply with federal guidelines to guard your nonpublic personal information against unauthorized access or use. We encourage you to help us protect your information and to keep your information accurate. The following best practices can be followed to protect your personal information.

Use Personal Information Only in Secure Transactions

- Financial transactions should only be conducted on secure websites. An indicator of a secure website is a URL that begins with “https” in the address, the “s” standing for “secure”. The “https” prefix should be on every page of websites used to conduct transactions, including the log-in page.
- Personal financial information (such as names in combination with social security numbers, account numbers, and credit or debit card numbers) and passwords for financial services (such as online and mobile banking) should only be used in secure transactions.
- Personal financial information and passwords for financial services should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications, or social media messages.
- Options such as “Remember me” or “Keep me logged in” on websites should be used sparingly.
- Personal financial information should never be sent by email in an unencrypted state.

Password Recommendations

- Passwords should use the maximum allowable number and a combination of characters such as upper- and lower-case letters, numbers, and symbols. Do not use easy to guess words, names, terms, or numbers.
- A different password should be used for each commercial and financial services website.
- Passwords that are written down or otherwise recorded should not be placed in visible or unsecured locations.

Approach Apps and Links on All Devices with Caution

- Approach all applications and links on all devices (personal computers, tablets, and cell phones) and delivery channels (email, text messages and social media sites) with caution, as cybercriminals often use applications and links as the first step in installing malicious software on devices with which fraudulent acts can be enabled.
- Take steps to verify that applications and links posted on social media sites correspond to legitimate websites, and that they have been posted by individuals who are known and trusted.

Secure Activity on Computers, Email, and Internet

- Install antivirus protection and scanning software that has been reviewed and rated as satisfactory by independent analysts. Your internet service provider may offer free anti-virus software for installation on your computer.
- If the security software can update automatically, set it to do so. If the security software cannot update automatically, update it after each login. Run a complete scan of your computer weekly.
- Operating system software updates or "patches" should be installed and run promptly to ensure you have the highest level of protection.
- Be wary of conducting financial transactions on computers that are shared by others in public places.
- Most Wi-Fi networks do not encrypt information and are not secure. Some use encryption and are more secure, WPA being common and WPA2 the strongest. However, if any Wi-Fi network is to be used, a virtual private network (VPN) should be established and used to encrypt communications. VPN encryption applies all the way from the user's PC to the host computer.
- Unfamiliar or suspicious emails, text messages, phone calls, websites and social media solicitations that request personal information should be deleted. They should not be replied to or forwarded. Do not click on links from unknown sources or ones that show up unexpectedly.
- Enable the firewall built-in to your computer to prevent unauthorized users from gaining access.
- Computers should be set to lock or log off automatically after fifteen minutes of non-use, with a password required to log back in. Turn off your computer if you do not plan on using it any time soon.

Avoid Payment Scams

- **Seller scams** request a payment in return for a phony service or product that you never receive. Types of seller scams include purchasing tickets and buying puppies.
- **Buyer scams** occur when a scammer pretends to "overpay" for a product you are selling, then asks you to pay the difference back to them.
- **Imposter scams** involve a scammer who poses as someone in authority like a sheriff; local, state, or federal government employee and demands a fast payment using Zelle® or a wire transfer. Call the government agency and ask if the person works for them before sending money.
- **Refund scams** occur when a scammer acts as if they owe you money and pretend to send you a higher, incorrect "refund" amount. They then ask that you return the "overpayment" using a method such as Zelle® or a wire transfer.
- **Payment app scams** involve a text or email that asks you to confirm a large, fake payment. If you reply to the message, the scammer may call you back and pretend to be a bank representative.
- **Gift cards or prepaid cards** should never be used for payments – such requests are signs of a scam.

Use Mobile Phones Securely

- Mobile phone applications, text messages, and calls from unfamiliar sources that request personal information and passwords should be declined, promptly deleted, and not replied to or forwarded. Any links should not be opened.
- Each mobile phone and mobile phone application should be assigned a different password with the maximum allowable number and type of characters.
- Verify your mobile phone will lock after fifteen minutes of non-use and that a password or PIN is required to log back into the phone.

- Mobile phones should be locked up when not in use and not left in visible, unsecured locations.

Use ATM, Credit, Debit and Prepaid Cards Securely

- Card numbers should only be used in secure transactions and should not be provided in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages.
- Card transactions should be conducted only on secure websites. An indicator of a secure website is a URL that begins with “https” in the address, the “s” standing for “secure”. The “https” prefix should be on every page of websites used to conduct transactions, including the sign-in page.
- Options to “Remember my card number” on websites where transactions are conducted should not be used.
- Cards that are unused, have been canceled or have been replaced by a new card should be securely eliminated, for example by cutting them into small pieces so they cannot be read.

Use Checks Securely

- Checks should not have social security or driver’s license numbers printed or written on them.
- Checks that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.

Statements, E-Statements, Bills, and Receipts

- Review or reconcile statements, e-statements, and bills promptly to verify all transactions were made by authorized parties. Banks, card issuers and billers should be notified in advance of a change of address.
- Statements, bills, and transaction receipts that are to be discarded should be eliminated securely, for example by shredding, and should not be discarded in a readable form.

Use Social Media Securely

- Use the highest level of privacy for social media sites. Do not allow social media sites to scan your address book. Accept only known and trusted individuals into your social network.
- Nonpublic information should be limited when using social media sites to prevent accounts from being compromised. Examples include personal financial information, passwords, phone numbers, email addresses, addresses and dates of significance such as birth dates and anniversaries.
- Nonpublic information also includes the names of financial institutions, commerce websites, internet service providers, utilities, and wireless carriers with which you have accounts.

Security Recommendations for Businesses

- Ensure computers are plugged into a network protected by a firewall. Limit administrative rights on computers conducting financial transactions.
- Use a standalone computer dedicated to handling financial transactions with tight user controls and no access to email or web browsing.
- Perform background checks on employees with access to financial accounts.