**For Immediate Release**

**For More Information:**

[Bank Contact

Contact Title

Contact Phone Number

Contact Email Address]

**[Bank Name] Provides Tips for Banking Online Safely and Being More Cybersecure***October is National Cybersecurity Awareness Month*

[Date] — Cyber-attacks are becoming more and more sophisticated and common. According to the 2017 Norton Cyber Security Insights Report, 143 million U.S. consumers were victims of cybercrime – more than half of the country’s adult online population – with losses totaling nearly $19.5 billion. In recognition of National Cybersecurity Awareness Month in October, [Bank Name] is highlighting tips and information to help consumers protect themselves from such cyber-attacks.

“The internet has become one of the most popular tools used to commit fraud and criminals are becoming more and more sophisticated with their hacking techniques,” said [Bank Executive Name and Title]. “As a result, customers must take the necessary precautions online, especially when using sensitive personal data such as bank account information.”

When banking online, [Bank Name] recommends that consumers take extra care to protect themselves by doing the following things:

* **Monitor your accounts regularly.** Make sure that all transactions posted are ones you have authorized. Report any suspected fraudulent or suspicious activity to your bank immediately.
* **Look out for strange emails!** Don’t respond to emails that claim to be from your bank (or any company) requesting your account details or passwords. Banks will not reach out to you over email to ask for your account details.
* **Avoid clicking links in emails.** It is usually much safer to log in to your bank website manually to ensure you are entering a secure site.
* **Change your bank passwords regularly.** Avoid using the same password across multiple sites and make sure you are choosing a strong password that is a mix of upper and lower case letters, numbers and special characters. Avoid using any words or phrases that contain your name, initials or your birthdate.
* **Enable two-factor authentication.** Many financial institutions have added a layer of security for account holders. Two-factor authentication requires you to enter an extra verification credential before you can access your account.
* **Disable automatic login.** Do not allow your web browser to store private username and password information for your online banking websites.
* **When available, only use your bank’s official mobile apps.** And make sure you download apps from reputable sources such as the Apple Store or Google Play Store.

[Bank Name] provides this additional information to help consumers to be more cybersecure:

* **Email fraud.** If it seems too good to be true, it is probably fraud. Don’t believe that lottery awards staff or princes from a foreign country will contact you by email!
* **Fraudulent payments.** Be on guard against fraudulent checks, cashier’s checks, money orders or electronic fund transfers sent with a request for you to wire back part of the money.
* **Unsolicited offers.** Be wary of unsolicited offers that require you to “ACT FAST”.
* **Stay up-to-date.** Make sure your device is up-to-date with the latest security updates for your operating system – Windows, Apple IOS, mobile phone IOS (Apple, Android, etc.).
* **Warnings and errors.** Do not trust websites with certificate warnings or errors.
* **Beware of email attachments.** It’s never a good idea to click on an email attachment or free software from unknown sources. You could end up exposing your system to online fraud and theft.
* **Sharing online.** Watch how much you share online. The more you post about yourself on social networking sites, the easier it may be for someone to use that information to access your accounts, steal your identity and more. Protect your personal information by maximizing your privacy settings.
* **Financial scams.** Be aware of disaster-related financial scams. Con artists take advantage of people after catastrophic events by claiming to be from legitimate charitable organizations when, in fact, they are attempting to steal money or valuable personal information.

Consumers are encouraged to report any suspected fraud to their banks immediately.

*About [Bank Name]*

[Bank boiler plate]

###