DATA PRIVACY DAY

is an international effort, **held annually on Jan. 28,**
to empower individuals and businesses to
respect privacy, safeguard data and enable trust.

Digital devices provide great convenience to our lives. Today, we are more connected than ever. By 2020, more than **30.7 billion** devices will be connected to the internet.

You are continuously generating data about yourself and others. Your personal information, such as your behaviors and preferences, is the fuel that makes these devices work.

YOUR PERSONAL INFORMATION IS LIKE MONEY – VALUE IT. PROTECT IT.

Here's what you can do now to manage your privacy:

1. **Create c0mplic@t3d passwords**. Avoid birthdays, pet names and simple passwords like 12345. It is also important to change passwords at least three times a year. Because friendly theft – theft by someone the victim knows – is the most common type of identity theft or fraud, don't share your passwords with family members and be mindful of who has access to your personal information.

2. **Keep tabs on your accounts**. Check account activity and online statements often, instead of waiting for the monthly statement. You are the first line of defense because you know right away if a transaction is fraudulent. Sign up for text or email alerts to be notified of transactions over a certain dollar amount or online transactions. If you notice unusual or unauthorized activity, notify your bank right away.

3. **Stay alert online**. Be sure computer and mobile devices are equipped with up-to-date anti-virus and malware protection. Never give out your personal financial information in response to an unsolicited email, no matter how official it may seem. Your bank will never contact you by email asking for your password, PIN, or account information. ONLY open links and attachments from trusted sources. When submitting financial information on a website, look for the padlock or key icon at the top or bottom of your browser, and make sure the internet address begins with "https." This signals that your information is secure during transmission.

4. **Protect your mobile device**. Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen. Before you donate, sell or trade your mobile device, be sure to wipe it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen. Use caution when downloading apps, as they may contain malware and avoid opening links and attachments – especially from senders you don't know.

UPPER PENINSULA
STATE BANK
You're going to like it here!