TIP 1:
Personal identifiable information, sometimes called PII, is some of the most valuable data that cybercriminals go after. With a Social Security number and birthdate, an industrious hacker could take control of nearly all aspects of your life, a co-worker's life or that of one of our clients.

With this much at stake, cybercriminals are turning to the keepers of this data — you and your co-workers — to gain access to PII. You need to know common tactics phishers use to lure users into giving up valuable PII. That's why we're sharing this infographic laying out what to look for to keep our company's and your data secure.

TIP 2:
Smartphones are the gateway into all sorts of data. From work emails to personal messages and information, access to your phone means access into your life.

Despite this, 28 percent of people don't secure their smartphones with any sort of passcode. Don't be one of them! Take the simple step of securing your phone with a passcode, pin or other security measure, such a fingerprinting or facial recognition. Keep it secure. Keep it safe.

TIP 3:
Passwords are part of all our daily lives. From paying bills to ordering pizza, nearly every web-based interaction requires a login and creation of a password.

With this many strings of numbers and letters needed, reusing passwords across multiple accounts can seem like an attractive option. But beware! Password reuse can turn one compromised account into dozens. Take some time to review the passwords you use and consider the following:

- Start using a password manager to wrangle all your various credentials for you.
- Turn on two-factor authentication on your accounts, or at least the most sensitive ones, such as email and banking.