

The background features a series of concentric circles in light gray, some solid and some dashed, creating a ripple effect. A large, solid red oval is positioned in the center-right of the frame. A dark gray, curved shape, resembling a stylized 'C' or a swoosh, is located to the left of the red oval, partially overlapping it.

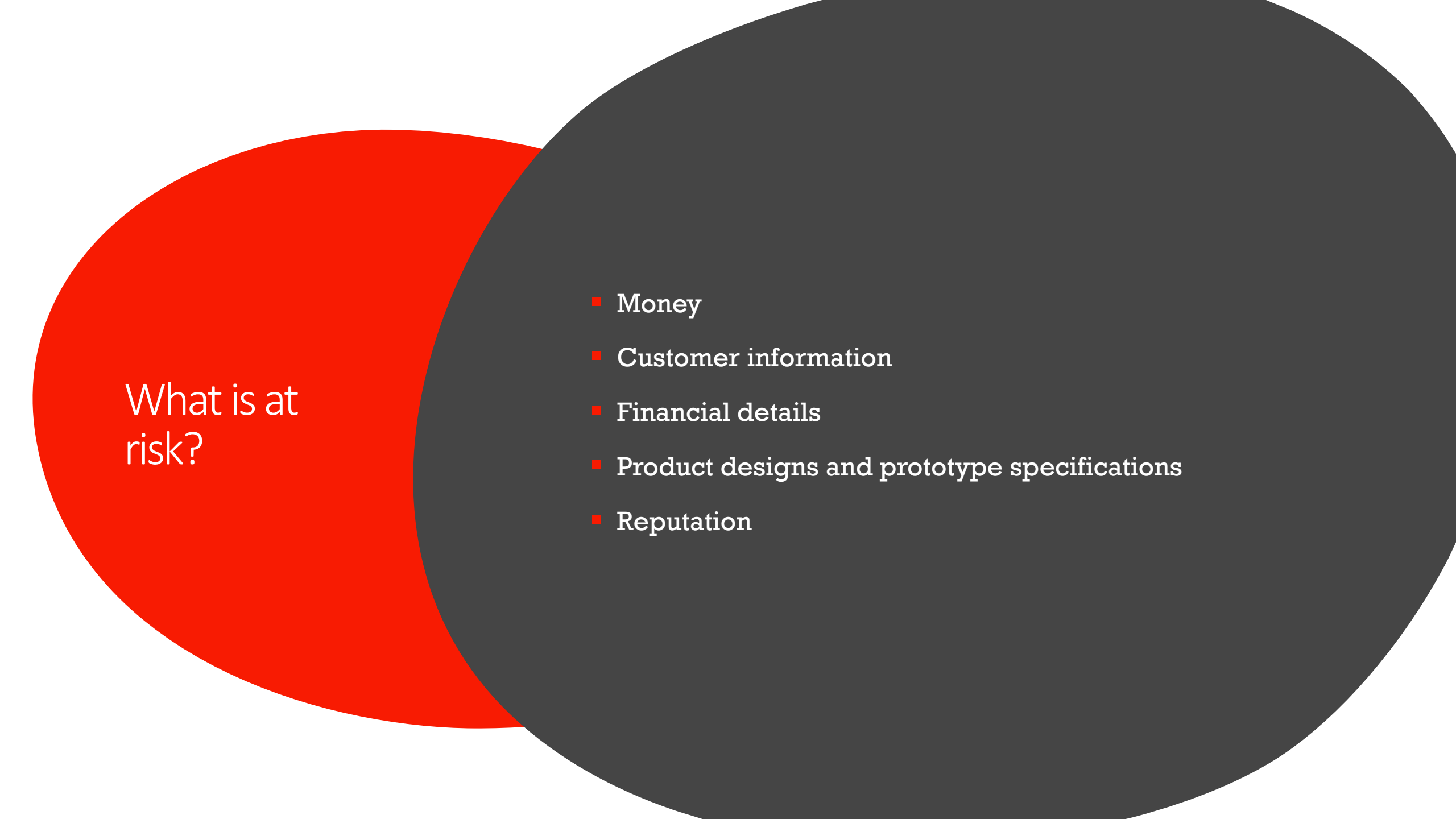
Risk Management

Data Security

Manage Risk?

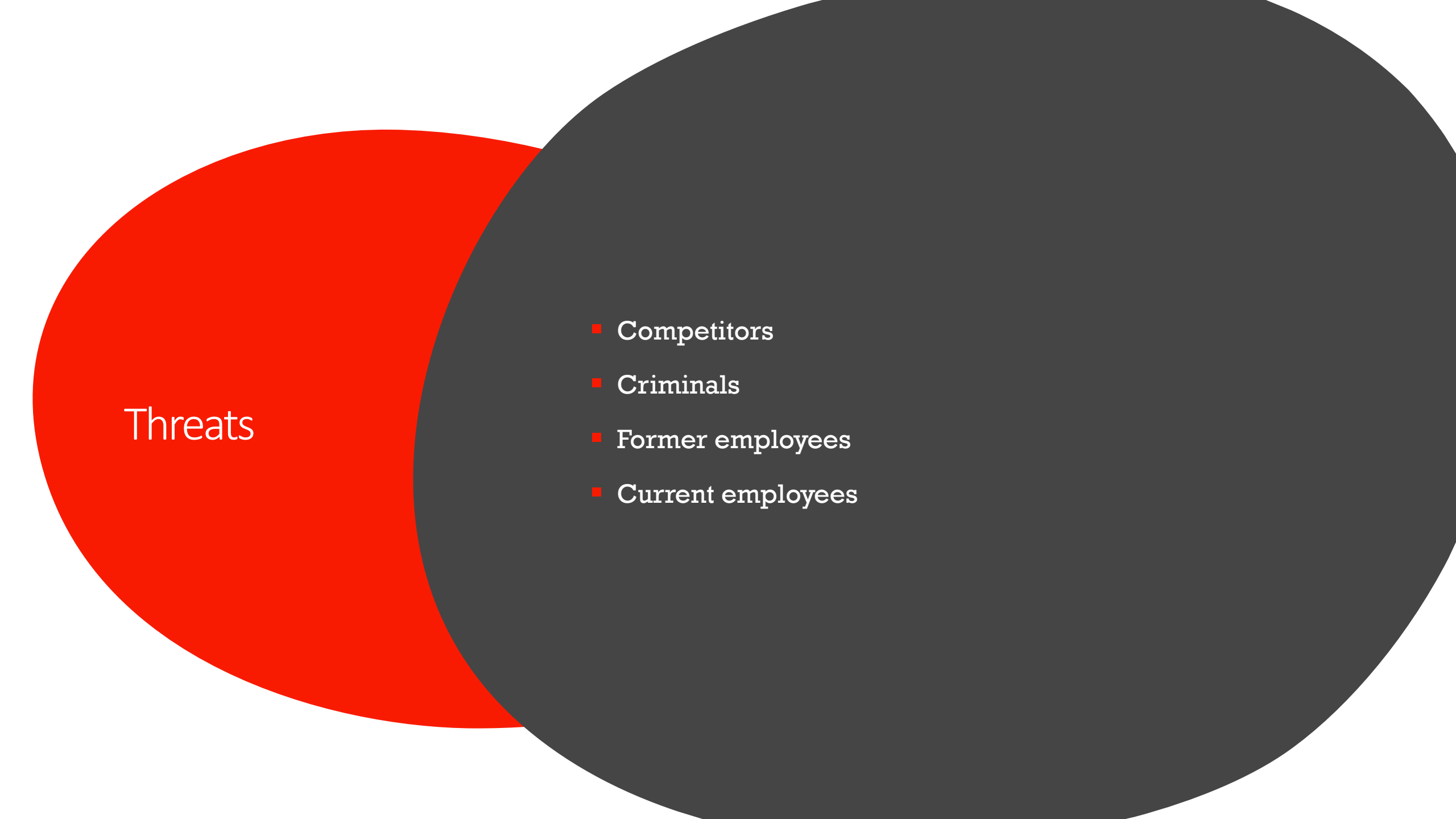
The aim of risk management in business is to reduce the associated risks to information assets and protect the business from cyber threats.

A business should know exactly what is at risk, what it holds that could be deemed valuable to a hacker and have a strategy in place to protect these assets.



What is at
risk?

- Money
- Customer information
- Financial details
- Product designs and prototype specifications
- Reputation



Threats

- Competitors
- Criminals
- Former employees
- Current employees

The background of the slide features several thin, curved lines in a light grey color, some solid and some dashed, creating a sense of motion or a stylized globe. On the left side, there is a large red speech bubble with a tail pointing towards the bottom left.

Government advice and support

The UK Government has a set of principles to support management of cyber security risks when making technology decisions.

These can be found [here](#):

<https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/get-basics-right-risk-management-principles-cyber-security>

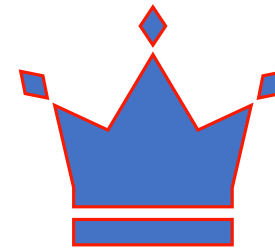
Crown Jewels

Every business has its own digital 'crown jewels'. Depending on the nature of the business, it could be media content, customer data, e-mail, product designs or other business-critical intellectual property that, if compromised or stolen, could severely undermine a business's reputation and revenues, or even destroy its ability to function.

These are the assets that drive cash flows, competitive advantage and shareholder value.

Therefore, protecting them should be of the highest priority.

Smaller businesses may not have the resources to protect everything they need to, but what they can do is put what they do have into protecting the 'crown jewels' of their business.



Risks associated with storing and sharing personal data

Are we sharing too much?

Facebook is the biggest social media platform on the planet, with over two billion people using it. Studies have shown that Facebook can predict your emotions, influence your emotions and it knows you better than your partner does, but, what if someone else, other than Facebook, had full access to that information. Sometimes they do, if your privacy settings are not set to only allow access to certain people.

We can also limit our exposure by being vague about what you post (where you are, where you are going, etc.), knowing your privacy settings on social platforms, and location settings on mobile devices.

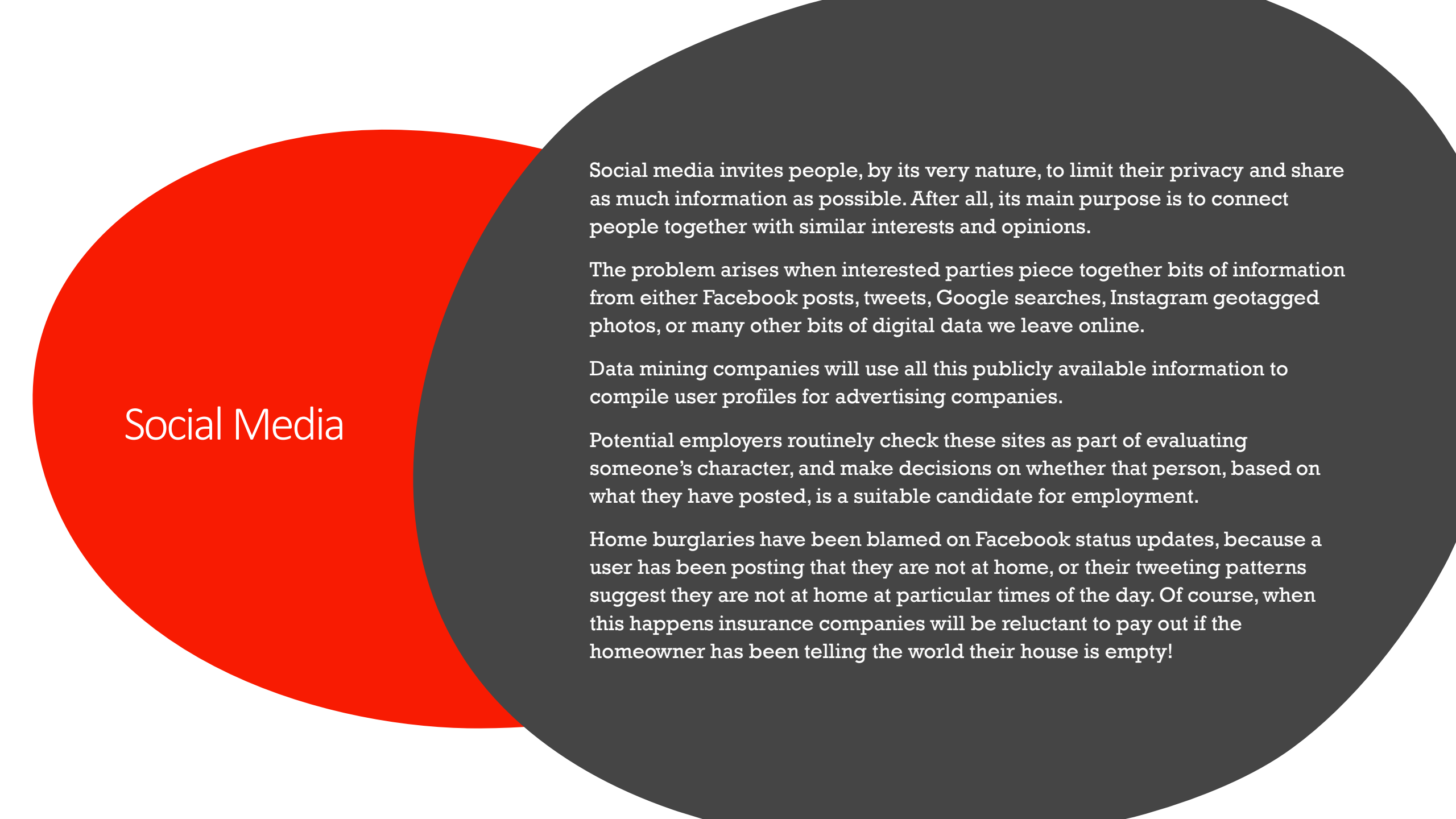
You may be careful about your digital footprint and what you post but what about what others post about you? Parents, friends, siblings? Their settings can determine who else can have access to your information.

Social Media Site	Number of Users
Facebook	2,603,000,000
YouTube	2,000,000,000
WhatsApp	2,000,000,000
Messenger	1,300,000,000
Weixin / WeChat	1,203,000,000
Instagram	1,082,000,000
TikTok	800,000,000
QQ	694,000,000
Sina Weibo	550,000,000
Qzone	517,000,000
Reddit	430,000,000
Kuaishou	400,000,000
Snapchat	397,000,000
Pinterest	367,000,000
Twitter	326,000,000

Social Media Users Worldwide*

(User Accounts)

*Source: statista.com 17 Sep 2020



Social Media

Social media invites people, by its very nature, to limit their privacy and share as much information as possible. After all, its main purpose is to connect people together with similar interests and opinions.

The problem arises when interested parties piece together bits of information from either Facebook posts, tweets, Google searches, Instagram geotagged photos, or many other bits of digital data we leave online.

Data mining companies will use all this publicly available information to compile user profiles for advertising companies.

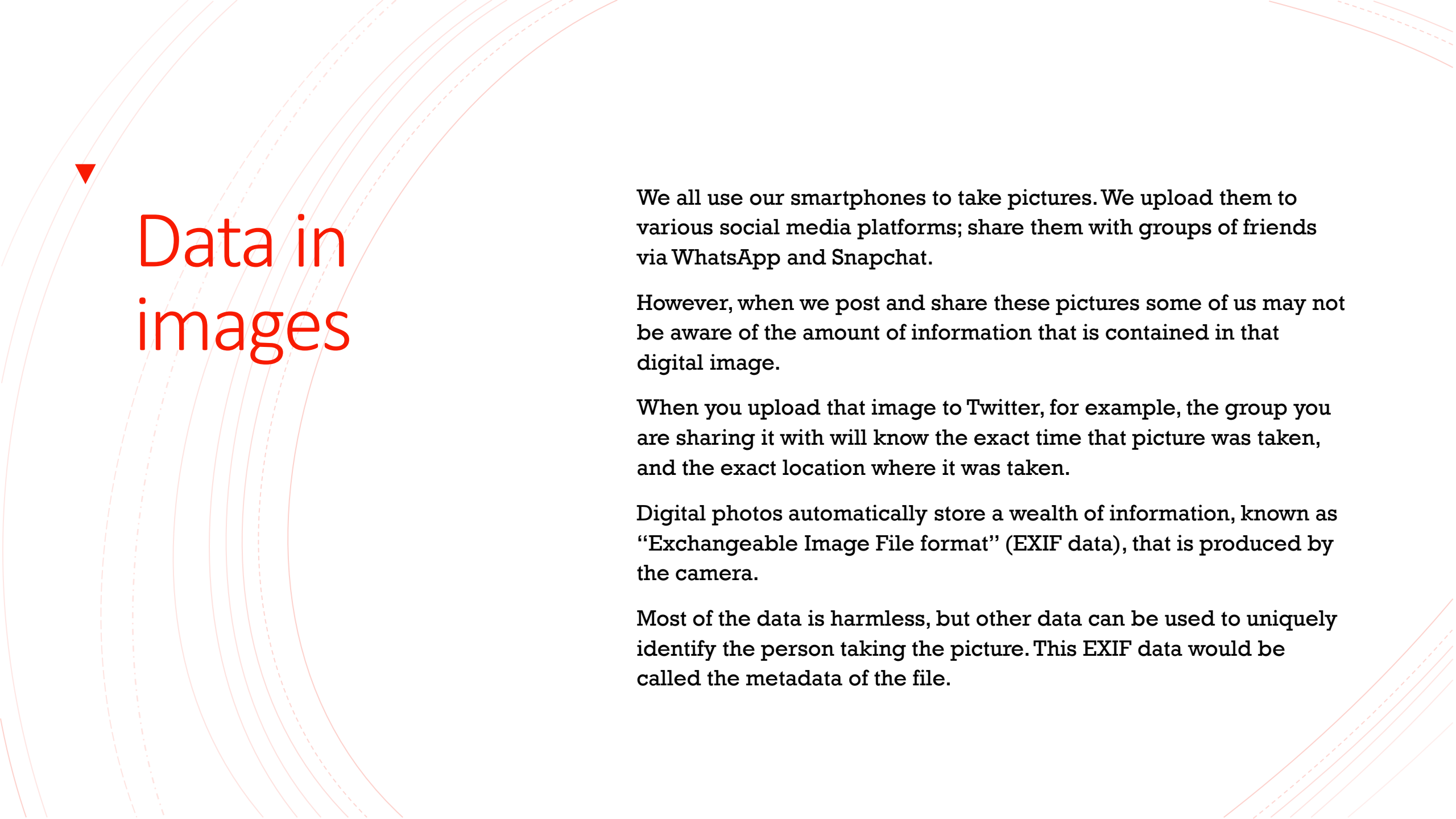
Potential employers routinely check these sites as part of evaluating someone's character, and make decisions on whether that person, based on what they have posted, is a suitable candidate for employment.

Home burglaries have been blamed on Facebook status updates, because a user has been posting that they are not at home, or their tweeting patterns suggest they are not at home at particular times of the day. Of course, when this happens insurance companies will be reluctant to pay out if the homeowner has been telling the world their house is empty!

Collection of browsing data

- Visit this web page to read about how companies collect your browsing data:

<https://www.reputationdefender.com/blog/privacy/how-companies-collect-your-private-information-when-you-browse-online>



Data in images

We all use our smartphones to take pictures. We upload them to various social media platforms; share them with groups of friends via WhatsApp and Snapchat.

However, when we post and share these pictures some of us may not be aware of the amount of information that is contained in that digital image.

When you upload that image to Twitter, for example, the group you are sharing it with will know the exact time that picture was taken, and the exact location where it was taken.

Digital photos automatically store a wealth of information, known as “Exchangeable Image File format” (EXIF data), that is produced by the camera.

Most of the data is harmless, but other data can be used to uniquely identify the person taking the picture. This EXIF data would be called the metadata of the file.

Metadata

Put simply, metadata is data about data. It is usually data contained in a file, hidden from the user, that allows a computer program to more accurately process information, ie what version of software you are using, how a file is encoded, who created the document, etc.

In the case of many popular image formats, such as JPG or TIFF, the list of possible metadata can be quite extensive.

- Aperture
- Shutter speed
- Focal length
- ISO setting
- camera make
- camera model
- Registration number
- Location data

A red speech bubble graphic with a white outline, pointing downwards. The word "Geotagging" is written in white text inside the bubble.

Geotagging

Geotagging is the process of storing the latitude and longitude data inside the EXIF data.

This will match the exact location of where an image was taken, and can be used with mapping services to pinpoint exactly where that location is.

Most people do not realise that the action of automatic geotagging takes place on their smart phones, either because it is enabled by default, not given to the user as an option, or an app asked for permission and then the user forgot to turn it off.

As a result, individuals often share too much information about their location, right down to the exact Latitude and Longitude when snapping photos with their smart phone and posting them online.

More info online

More information online: click the hyperlink

- [Geotagging on Android phones](#)
- [Geotagging on Apple phones](#)

With all the data we put out about ourselves, we are putting ourselves at risk – risk of identity theft, damaged reputations, cyber bullying and social engineering.

Cyber Hygiene



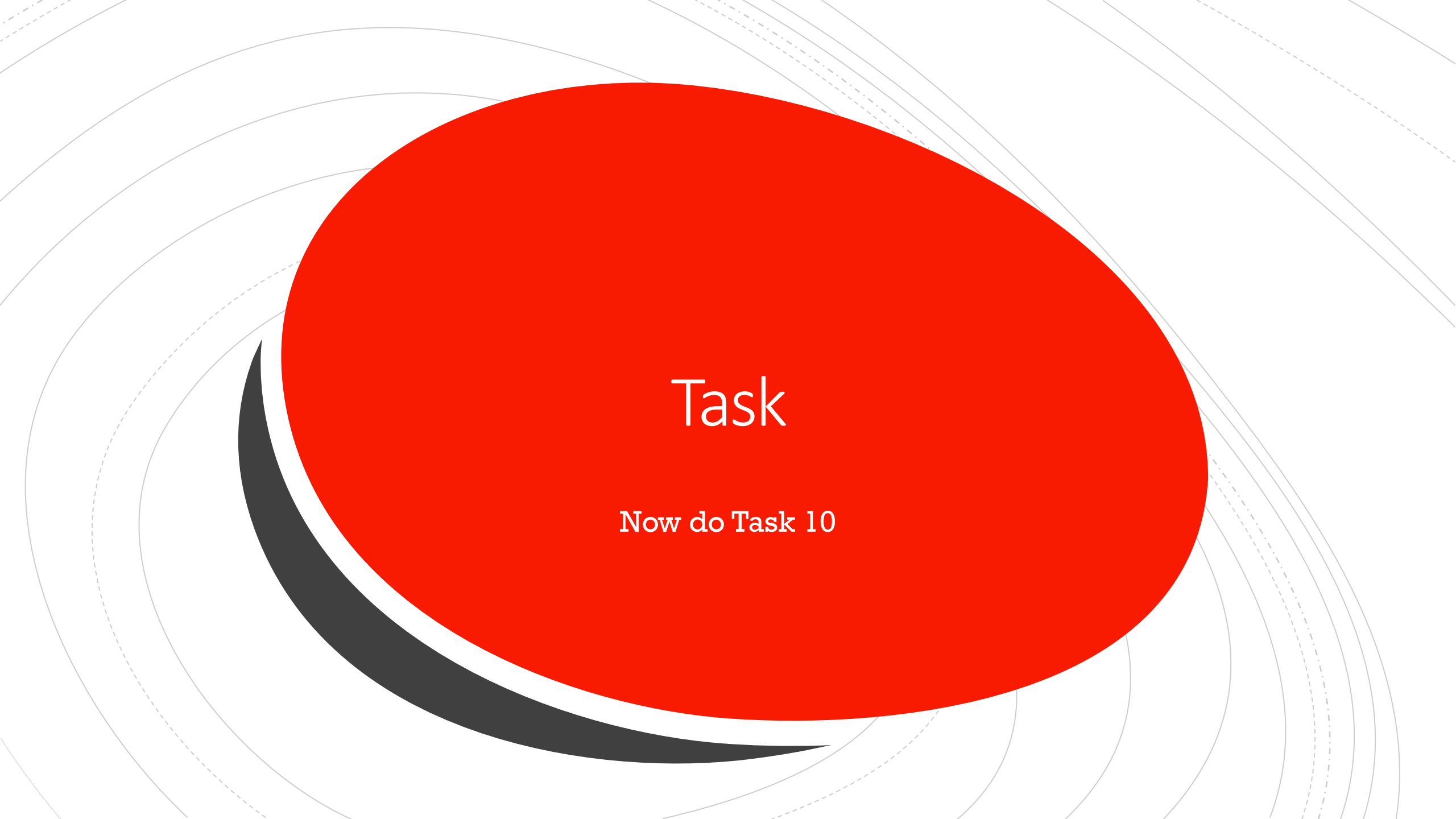
Having good cyber hygiene can limit the risks that we face online.



As we have seen, sharing too much information can lead to someone else getting access to your information.



Passwords can be guessed, for example, if your security question to your account is “pet’s name” and your social media feeds are filled with pictures and updates of your pet!

The background features a series of concentric circles in light gray, some solid and some dashed. A large, solid red oval is positioned in the center-right of the frame. A dark gray, curved shape, resembling a thick comma or a stylized 'C', is located to the left of the red oval, partially overlapping it.

Task

Now do Task 10