K2's Privacy Issues & Solutions - *What You Need To Know!*

K2 Enterprises

Learning Objectives

Identify examples of critical privacy threats

Cite examples of how your data becomes compromised through web browsers and search engines

List maneuvers you can make to reduce your privacy risk

INTRODUCTION

Introduction

- In an increasingly connected world, **all our personal information is under siege**, and there are few boundaries yet to be crossed
- Your **browsers, search engines, the web sites you visit, and the merchants with whom you do business all represent potential exposure points** of sensitive and personal data
- **As individuals, we *should* be concerned** about this issue
- **At a corporate level, we *must* be concerned because of privacy laws and regulations**

Privacy Versus Security

What Is The Difference?

- Some view **privacy** and **security** as the same issue
- Although similarities exist, **these topics are, indeed, different**
- For today's discussion, we will view **privacy as the right to control your personal information and how others use it**
- On the other hand, we will view **security as the methods and techniques used to protect your information**

Examples, According To Norton

- **Both privacy and security are maintained**
  - Bank uses data you provide to open your account and they protect that data from unauthorized access or use
- **Privacy is compromised, but security isn't**
  - Bank sells your personal data to marketing company with your consent, even though you may not realize you consented
- **Both are compromised**
  - Bank suffers a data breach, and because of this breach, your personal data – Social Security number, for example – is compromised

Other Examples

- Your **web browser tracks all the sites you visit** and uses this information to develop marketing profiles about you
- Your **search engine records all the phrases you search for** and compiles a dossier about you
- An **ecommerce web site from which you purchase products creates and maintains a database of items you purchase** and uses this data to make product suggestions to you
- Keeping all the above in mind, **how many organizations already have significant amounts of data collected on you**?

PRIVACY POLICIES – THE FINE PRINT

Privacy Policy Issues

- Many of our privacy issues can be traced back to privacy policies and individuals not taking the time to investigate how their data is collected and used
- More specifically, **end users generally do not read the "fine print"** and, therefore, fail to understand the implications of their choices to use specific browsers, search engines, services, etc.
- Let's consider two examples…

A Portion From Google's Privacy Policy

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

A Portion From Google's Privacy Policy

When you're not signed in to a Google Account, we store the information we collect with unique identifiers tied to the browser, application, or device you're using. This allows us to do things like maintain your preferences across browsing sessions, such as your preferred language or whether to show you more relevant search results or ads based on your activity.

When you're signed in, we also collect information that we store with your Google Account, which we treat as personal information.

You Can See What Google Knows…

- Curious about what Google knows about you?
- Use **Google Takeout** to download a copy of what Google has on file about you (https://takeout.google.com)
- Note, using Takeout doesn't delete the data!
- If you want to delete, visit https://myactivity.google.com

Another Example - Intuit

Here's what we mean by "platform" – when you choose to share data with us, or bring over information from third parties (like a bank or loan provider), we use that data together, not just within the individual offering(s) you're using. This means your bookkeeping details from QuickBooks, budgets from Mint, and recommendations from Credit Karma all live together….. Keeping your data in one place like this enables us to save you time by putting the information you choose to share with us to use. For example, if you ask us to, we can fill out a loan or credit card application for you based on what we already know about you.

THE FIRST STEP TOWARD PRIVACY – READ AND UNDERSTAND PRIVACY POLICIES!

YOUR BROWSER AND SEARCH ENGINE MATTER AND WHY THEY MATTER

Privacy Issues With Browsers

- The **most commonly-used browsers today potentially pose significant privacy risks**
- You can **mitigate some of these risks by adjusting settings** within the browser
- Alternatively, you can **change to a browser that is potentially more secure** to help protect your personal information

Examples Of Browser Risks

Some of the general risks include:

- **Browser fingerprinting**
- Malware
- **Tracking cookies**
- **Pop-up ads**
- Browser extensions and plug-ins
- Cross-site scripting

Browser Fingerprinting

- **Browsers might send information about your computer to the sites you visit**
- Included in this information are items such as
  - Browser type and version
  - Your computer's operating system
  - Time zone
  - Language
  - Screen resolution
- Some of these items can improve your "experience"
- Others can present privacy issues

Tracking Cookies

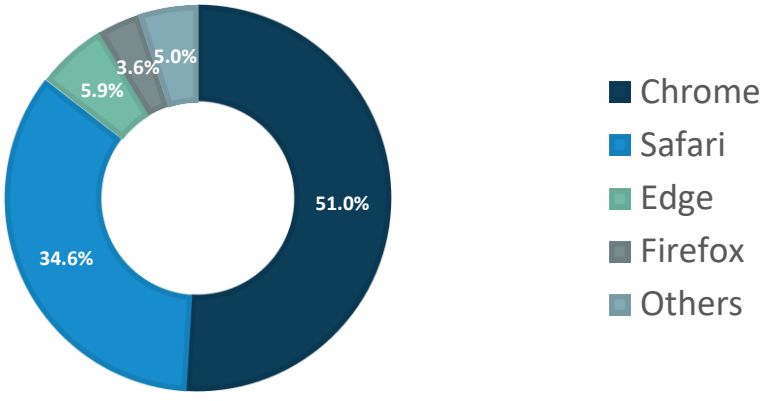
- **Cookies collect data about you and this data can be used to add or enhance functionality** – such as shopping carts – on a web page that you are visiting
- However, **cookies can also be used to send targeted ads or other forms of content**, without you requesting that information
- In addition, they can **track and send information such as your location, purchases you may have made, the ads you looked at, and how long you looked at an ad**
- This **info can be compiled into a dossier and then sold to other companies** to enhance their marketing efforts

Pop-Up Ads

- In concert with cookies, **pop-up ads can collect information about you, including whether you clicked on the ad**
  - If you clicked on the ad, you presumably are interested in the product or service and that information is used for additional marketing efforts
- Pop-up ads **can also present security risks in the form of encouraging viewers to click on the ad and, upon doing so, infecting the computer with some form of malware**

Browser Market Share

North America, Through January 2022

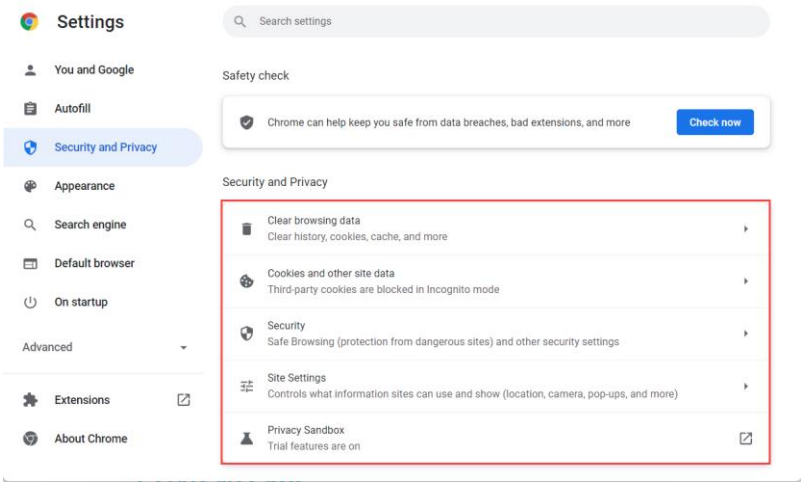


CONFIGURING BROWSERS FOR PRIVACY

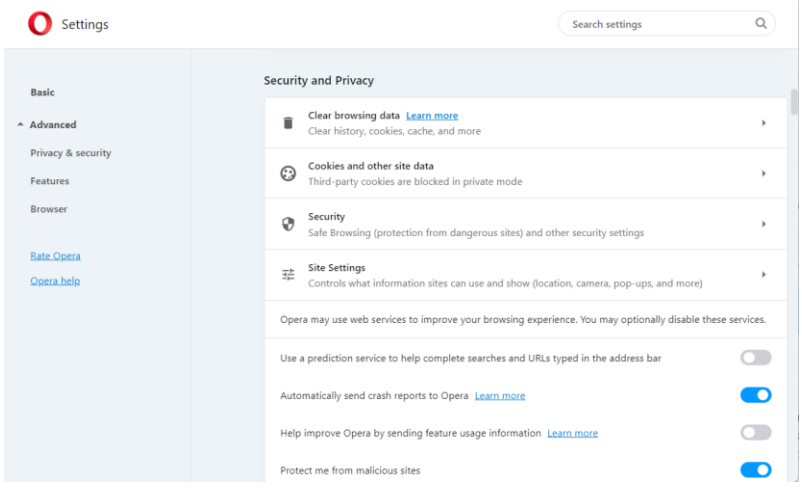
Browser Privacy Settings

- In general, **most browsers install with few privacy settings enabled by default**
- However, if you know where to look, **you can strengthen those settings and protect personal information**
- See the article at https://tinyurl.com/bmymackn for recommendations on a browser-by-browser basis

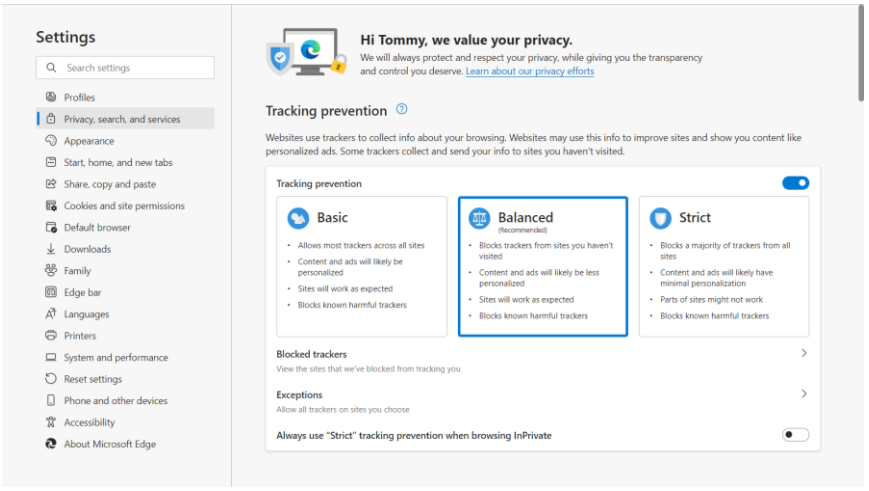
Making Chrome More Private



Making Opera More Private



Making Edge More Private



DO WE REALLY WANT TO DEPEND UPON END-USERS TO CONFIGURE BROWSERS?

Maybe A New Browser Is In Order

- **Brave**, a relatively new browser option, **provides a very robust set of privacy options enabled by default**
- As examples**:**
  - **Blocks all ads and trackers** by default
  - **Brave uses "fingerprint randomization"** so you appear different to every site you visit, each time you restart the browser
  - Brave **blocks third-party cookies and third-party storage**
  - Includes optional features to **block social media and browsing through Tor servers** to prevent others from seeing where you've browsed, among others

DON'T FORGET ABOUT PRIVACY ISSUES IN SEARCH ENGINES

Search Engine Privacy Issues

- Most **popular search engines – including Google – track and collect significant amounts of data**, by default
- However, you do have **options to improve privacy**
- For example, **DuckDuckGo** provides excellent search capabilities, with the following benefits
  - **No tracking**
  - **No targeted ads**
  - **Results are not based on search history**
  - **Fewer ads**

SHOULD YOU USE A VPN TO IMPROVE PRIVACY?

VPN's – A Primer

- **Virtual Private Networks (VPNs) provide a secure, encrypted tunnel** through the otherwise unencrypted internet, helping to ensure security and privacy of sensitive information
- When connected to the Internet through a VPN, **you reduce the risk that others can see your traffic**
- Accordingly, **browsing through a VPN provides an added layer of privacy** and helps to protect sensitive information
- In addition, **VPN's can facilitate secure remote connections to other computers**

VPN And Privacy

- If you are **connecting to the web from within your corporate network, there is a high probability that you have the protection of a VPN enabled by your IT staff**
  - Of course, verify!
- On the other hand, **if connecting from outside the network – such as from home – you could benefit from a VPN solution**, more specifically a **Remote Access VPN**

VPN And Privacy

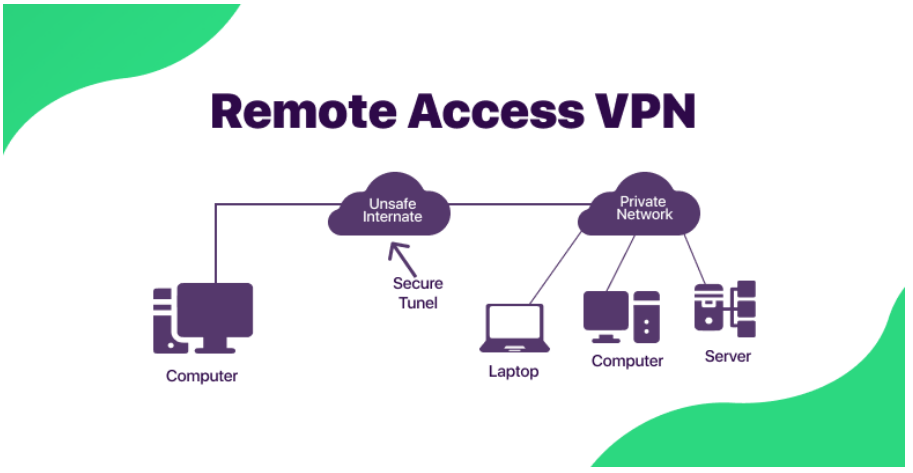


Image courtesy of PureVPN

PC Magazine's Top Ten VPNs

- Proton VPN
- NordVPN*
- Surfshark VPN
- Private Internet Access VPN*
- CyberGhost VPN
- TunnelBear VPN
- ExpressVPN
- IVPN
- Mullvad VPN
- Mozilla VPN

In general, pricing typically runs under $6 per user, per month
**=may have foreign bad actor risk based on reporting*

Summary And Wrap-Up

- **Privacy issues abound for us business professionals and also as consumers**
- The ability for **organizations to collect and analyze massive amounts of data can indeed improve consumer experiences**, but at what cost?
- We must do a **better job as individuals in understanding the issues and, at an organizational level, in handling the data**
- Fortunately, the tools are there; **we just need to take advantage of them!**

tommy@k2e.com

THANKS FOR PARTICIPATING TODAY!