The Cyber Exchange
The Dark Web

By Dan Struthers
HardSoft Systems Ltd
www.hsl.ca

WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs · MACS · ANDROID TABLETS · SMART PHONES

Passwords
- Web browser autofill
- Stored in the file system

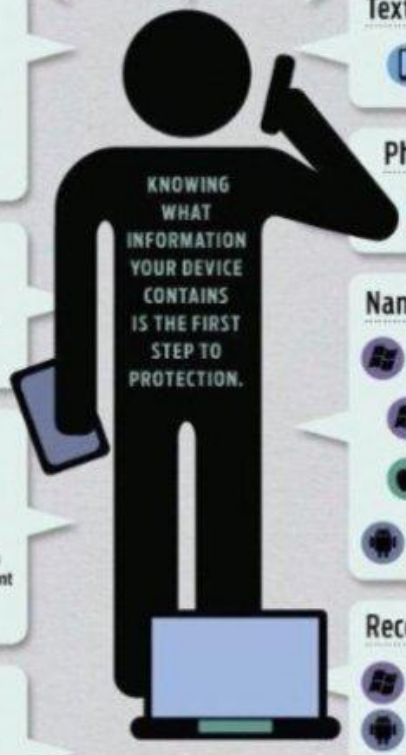
Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

Social Security Number
- Downloaded tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log stored on phone



Bank Account Info
- Downloaded bank statements

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Recent Files
- List kept by operating system
- Various applications keep their own recent file lists

Recently Visited Sites
- Browser's cache
- Browser's history
- Cookies

Contacts
- Windows Contacts
- Address Book
- Contact manager

Current Location
- Readable off your GPS

Recent Locations
- Photos
- Navigation apps

Statistics

- Retail exposed 67% (420M) of the number of records in the total dataset.
- Companies with less than $50M in revenue were the most impacted, accounting for 47% of the claims.
- The average total breach cost was $394K, the median $56K.
- Companies with revenues greater than $2B suffered an average breach cost of $3.2M.

How Are Credentials Compromised?

Phishing

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials

Malvertising

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials

Watering Holes

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials

Web Attacks

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials

Federal Financial Institutions Examination Council (FFIEC),
"Joint Statement: Cyber Attacks Compromising Credentials", March 2015

HSL

ID AGENT

Typical price range on Dark Web markets for compromised credentials, ranging from online services to corporate network usernames and passwords

$1-$8

HOW OFTEN ARE DIFFERENT TYPES OF PII INVOLVED IN DATA BREACHES?*

Contact Information  89%

Financial Details  42%

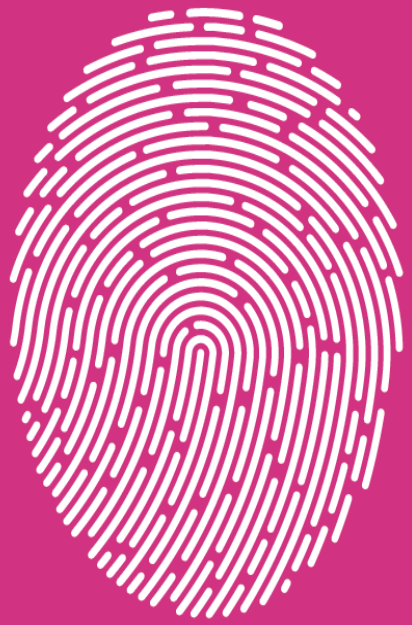
Identity Information 

39%

Health Information  25%

Source: Australian Government *Based on Australian Businesses

What Can an Attacker Do with Compromised Credentials?



- Send Spam from Compromised Email Accounts
- Deface Web Properties and Host Malicious Content
- Install Malware on Compromised Systems
- Compromise Other Accounts Using the Same Credentials
- Exfiltrate Sensitive Data (Data Breach)
- Identity Theft

9 WAYS YOUR EMPLOYEES' WORK CREDENTIALS CAN LEAD TO A BREACH

When your employees use their work email on websites like the ones listed below, it makes your business vulnerable to a breach. With our Dark Web Monitoring, we can detect if your company is at risk due to exposed credentials on 3rd party websites.

HR & PAYROLL

ADP, Payworks, PAYCHEX, canadian payroll systems

EMAIL SERVICES

Office 365, YAHOO!

CRM

salesforce, HubSpot, ZOHO

TRAVEL SERVICES

Expedia, travelocity, ORBITZ, FASTBOOKING

COMMUNICATIONS

ROGERS, Virgin mobile, Bell Aliant, Shaw

E-COMMERCE

amazon, STAPLES, Dennis, ebay

BANKING & FINANCE

QuickBooks, freshdesk, RBC, Scotiabank, TD

COLLABORATION

Dropbox, box, CITRIX

SOCIAL MEDIA

UNDERSTAND & MITIGATE YOUR RISK

EXTERNAL THREAT INTELLIGENCE	DATA BREACH & PRIVACY LAW COMPLIANCE	# OF EXPOSED CREDENTIALS FOR YOUR COMPANY IN THE PAST 36 MONTHS
Are you monitoring for compromised data that can be used to exploit your business? ☐ YES ☐ NO	Do you have a compliant data breach response plan in place? ☐ YES ☐ NO	_____

Email addresses and passwords

600K Facebook accounts are hacked daily

- 50% of users use the same password for everything

- At least one person will
- click on everything

Sample Report of Dark Web Monitoring

Date Found	Email/IP	Password Hit	Source	Type	Website
10/4/2018	johndoe@yourcompany.ca	form****	id theft forum	Not Disclosed	bell canada
10/4/2018	janedoe@yourcompany.ca	fire****	id theft forum	Not Disclosed	edmodo.com
9/29/2018	joe.employee@yourcompany.ca	Vinn**	id theft forum	Not Disclosed	Not Disclosed
9/25/2018	anyemployee@yourcompany.ca	berl******	id theft forum	Not Disclosed	fashionfantasygame.com

Find out BEFORE the damage is done

Thank you

Dan@hardsoft.ca
www.HSL.ca

800 263 8433