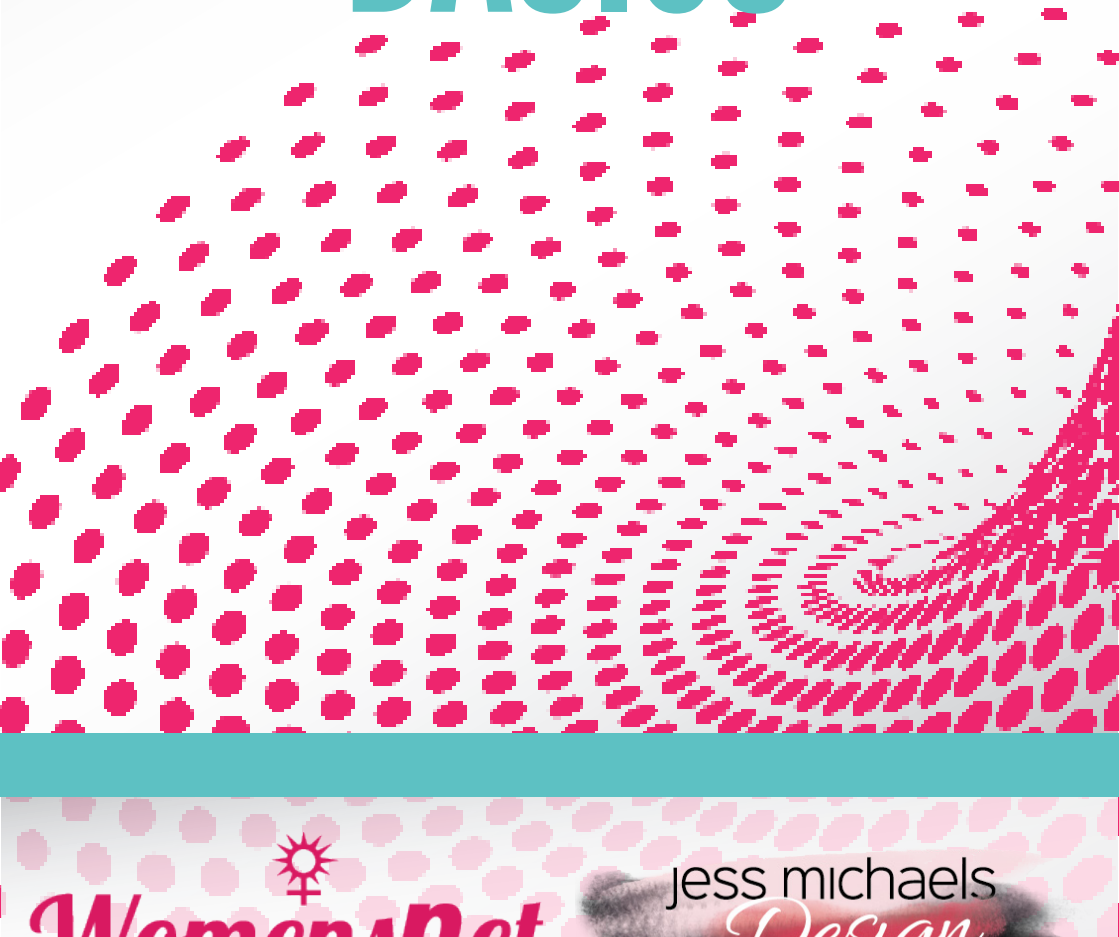
CYBER SAFETY BASICS



WomensNet

jess michaels Design

TABLE OF CONTENTS

IS THE INTERNET DANGEROUS?

The short answer is: “it can be“.
The long(er) answer is that “it doesn’t have to be“.

Much like the real physical world, the internet is a vast enough place to harbour various dangers, which should not pose a threat if you are equipped with enough knowledge to combat them. Luckily, this is what this booklet is here to help you with!

WHY USE THE WEB?

But if the internet is such a threatening place, why bother exploring it?

There is so much that you can gain from using the internet. It is a massive resource that can enrich any aspect of your life once you know how to navigate it safely.

Read on to learn all you need to know to stay safe in cyberspace.

WHAT IS A SAFE WEBSITE?

A key factor in staying safe on the internet is ensuring the website you're on is not dangerous. Fortunately, there are of ways to identify a site that is safe, and, conversely, one that may be dangerous.

WHAT IS A DANGEROUS SITE?

In this case, we'll say that a dangerous website is one that may:

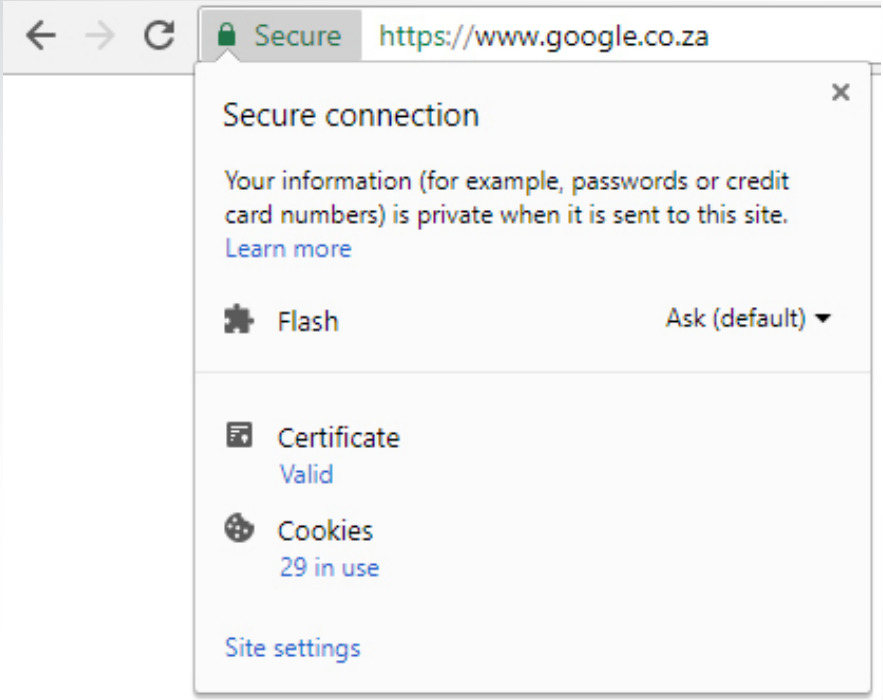
- Steal your information
- Download unwanted software onto your device
- Leave you vulnerable to hackers

HOW TO IDENTIFY A SAFE SITE?

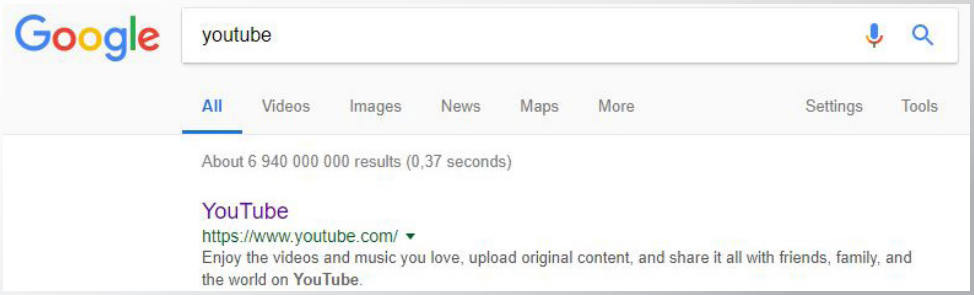
Here are some ways that can help us identify a safe website:

1. Look for some signal that your browser knows a site is secure. In Chrome, it looks like this:

If you click on the green “secure“ text, Chrome will tell you how you are safe.



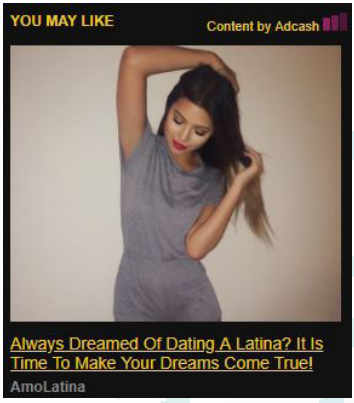
2. Big, recognisable brands like Facebook, Twitter, Google and YouTube are expected to be safe for browsing. If they weren’t, their users and thus their source of income, would not want to use their product.
Remember to use the correct web addresses; you can generally find this as the first result of a Google search.



HOW CAN WE SPOT A DANGEROUS WEBSITE?

Although not all dangerous websites will have these characteristics, some may display one or more of them:

1. Plenty of ads, especially ones advertising pornography/dating sites that objectify women, gambling, and weight loss/anti-ageing “miracles“, or ads that open in a new window (pop-ups) or that are otherwise intrusive.



The websites that these ads are being displayed on may be safe, but if you were to click on one of these types of ads, they may lead to a dangerous website. It’s best to assume that any kind of website that would allow these ads on it may not be the most reputable.

2. Typographic errors are often a sign of a website that doesn’t care much for its quality.

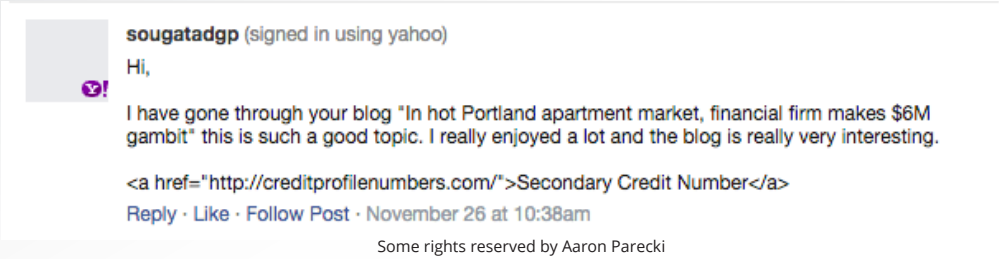
3. Look for strings of semi-related words in poorly formed sentences, or sometimes not even sentences at all. This is called “keyword-stuffing“, and it’s something that some websites do to try to trick search engines into ranking them as highly as possible, without putting in the work to produce valuable content.

2,798 blog reactions to **Darren Barefoot - Vancouver Technologist, W**

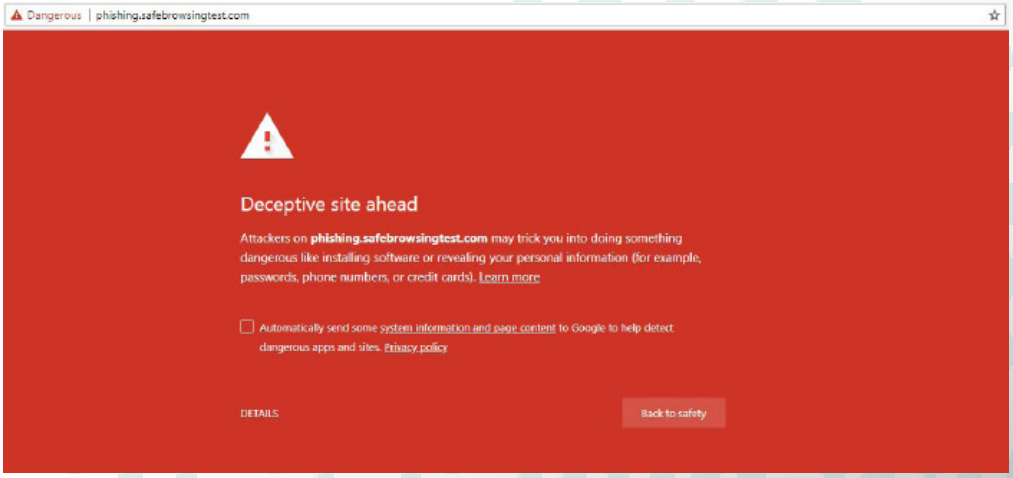
BlackHat Planet - internet marketing, seo, internet marketing online, seo services, internet marketing tool, dw230 seo, internet marketing strategy, company seo, internet marketing services, internet marketing advertising, seo tool, search engine optimisation, ppc search engine internet marketing, engine optimization search seo, consultant michigan seo, business driven michigan seo technology, internet marketing company, internet marketing consultant, optimization seo, internet marketing book, internet marketing solution, michigan seo solution, internet marketing business, design seo web, firm seo, expert seo, seo technology, environment seo technology, design michigan seo web, strategic internet marketing, michigan seo, consultant seo, internet marketing seo, internet marketing ebook, michigan ohio seo, marketing seo, business home internet marketing opportunity, internet web site marketing, seo training, home based internet marketing business, web internet marketing, seo software, marketing seo target, seo service, real estate internet marketing, internet marketing search engine, affiliate internet marketing, internet marketing affiliate program, article seo, internet marketing consulting, internet marketing for small business, internet marketing course, engine promotion search seo software strategy, internet marketing search engine placement, copywriting seo, dw230 seo ????, expert from insider internet making marketing millions online secret story success today who, seo site web, internet marketing firm, seo toolbar, michigan seo technology, book seo, marketing michigan seo target, internet online marketing advertising business, online business internet marketing computer, internet marketing center, web site promotion internet marketing, internet marketing guide, internet marketing toronto, denver internet marketing, internet marketing online advertising, dw230 seo ???, dw230 seo ??, home business internet marketing, internet marketing chicago, internet marketing specialist, inc seo, affordable seo, business internet marketing opportunity, consulting seo, 3g edition generation internet internet marketing marketing online seventh strategy success third, estate real seo, internet marketing agency, seo toronto, internet marketing resource, elite seo,

4. Large, attention-grabbing buttons telling you to download something may be trying to trick you into downloading malware.

5. Look out for websites that allow spam comments. These kinds of comments will often be nonsensical, have non-standard characters, link to non-reputable sites, or try to advertise pirated movies.



6. Modern web browsers are often programmed to identify a dangerous website and warn you before you enter it. For example, if you're using Google Chrome, this warning will appear, and you can easily navigate back to safety.



PERSONAL INFORMATION

Personal information entails passwords, ID numbers, all debit/credit card information, addresses, phone numbers, account numbers and any other information that may be used to access any account of yours.

WHY SHOULD I KEEP THIS SAFE?

Anybody with access to your personal information could also access accounts such as:

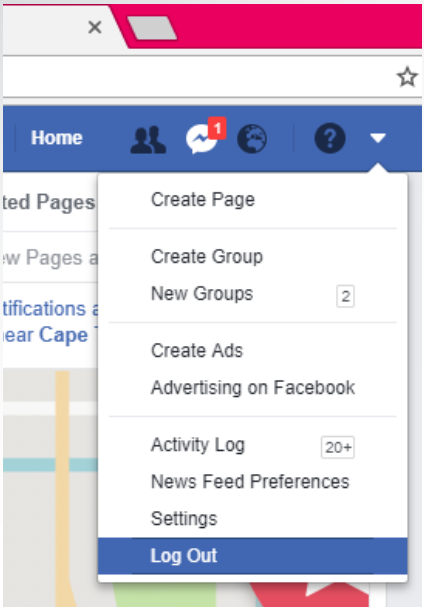
- Bank accounts
- Social media accounts
- Email inboxes
- Store accounts

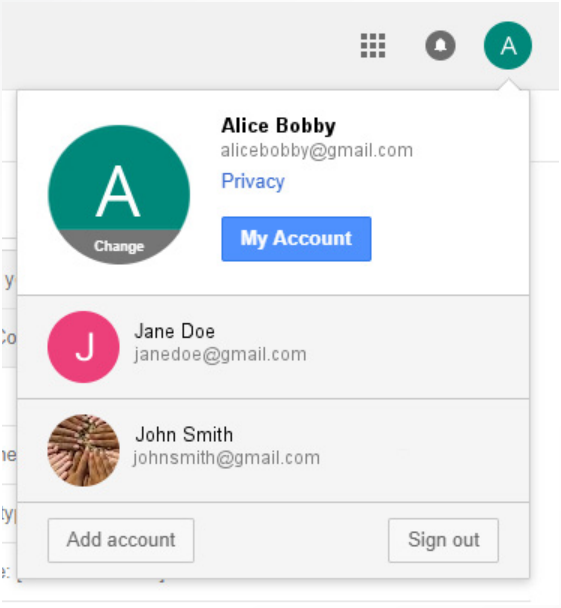
As you could probably guess, you definitely do not want strangers to access this, or they could steal your money or your identity.

HOW CAN I KEEP MY INFO SAFE?

First and foremost, never tell anybody, unless you are 100% sure you can trust them. Other ways to stay safe are:

1. Always log out of all accounts after using a computer that is not your own.





2. Always check that the web address you are trying to log in from is correct.

3. If you are going to write down your password, keep it in a safe place that only you and the people you trust have access to.

4. Try to have a different password for every account.

5. Companies and businesses will never ask you to send them your password in an email or telephone call.

6. If you suspect that your account has been hacked, change your password and/or contact the website support team.

HOW DO I CREATE THE SAFEST PASSWORDS?

Never choose an obvious password, such as (or similar to):

- “123abc”
- “p@ssword!”
- Your spouse, partner, child or pet’s name
- Your birthday
- Your favourite TV show character, celebrity, etc
- “hijklmnop” or any consecutive letters of the alphabet
- “aaa“ or any character that is repeated consecutively

The best passwords have a combination of uppercase letters, lowercase letters, numbers and symbols. Not only does this make it difficult for people to guess, but it also makes it less likely that hacking software can guess it.

7bWkj!qU$9!8=yn?

ONLINE SHOPPING AND BANKING

Shopping and banking online is safe, efficient and time-saving — if you do so on a trusted website.

Thanks to this handbook's chapter on safe websites, you should be better equipped to identify one that can be trusted. However, when money is involved, there a few additional things to be aware of.

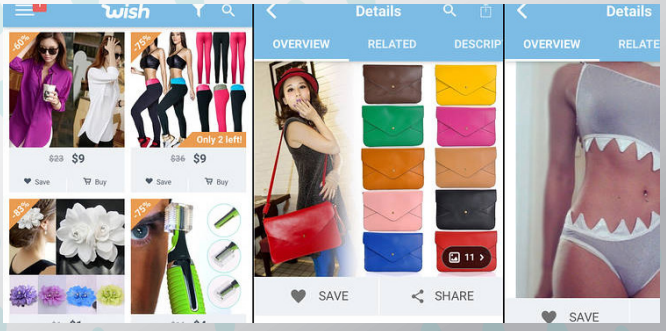
ONLINE SHOPPING

When shopping online, remember to be aware of the following:

1. Stick to established websites, such as Amazon and Takealot.

2. If you're unsure of a site's reputation, search for reviews on Google.

3. On websites with wholesale sellers selling heavily discounted goods (such as Wish or eBay), always carefully inspect images, descriptions and product reviews to ensure that they are not falsely representing their goods. If there is a problem with your purchase, you can message the seller to replace the item or refund you; if they refuse you should be able to report the seller to the website support team.



4. Ensure that the website uses a secure method of payment. PayPal or i-Pay Instant EFT are secure. If the eCommerce website is a well-established brand, they can be trusted to use a secure means of payment. Also ensure that your browser recognises that the site is secure (refer to page 3).

ONLINE BANKING

Banking online is designed and developed to be 100% secure. However, ensure the following:

1. The website that you are trying to bank from must be the correct one, with the correct address.

2. You can ask at your bank for help with setting up and navigating your online banking profile.

3. Use a different password for your online banking profile than your other accounts, and don't save the password to your browser if prompted.

EMAILS

Emails are still a very popular means of communication online. While most email software and services have become smarter in detecting harmful and unwanted content, you should still be aware of the following:

1. Do not fall victim to scams. Emails from people you don't recognize claiming to offer you money or inheritance, or from small "companies" offering web design and marketing services are examples of scam emails.

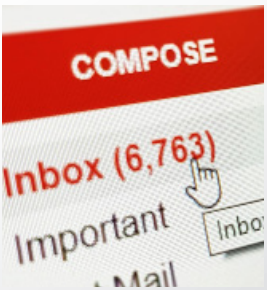
2. If you no longer want to receive correspondance from a company, there should be an "unsubscribe" link either at the top or bottom of the newsletter.

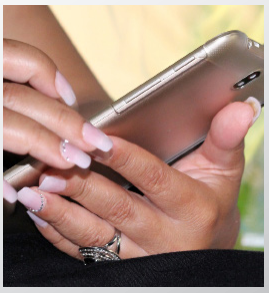
3. If your email software has not identified a spam or scam email as such, you can flag it or block the sender. If you don't know how, look for help documents online.

4. Don't click on links from senders you are not familiar with.

5. Similarly, don't download attachments from senders you don't trust.

6. Don't feel like you need to respond to every email you receive. Use your best judgement when engaging with an email.



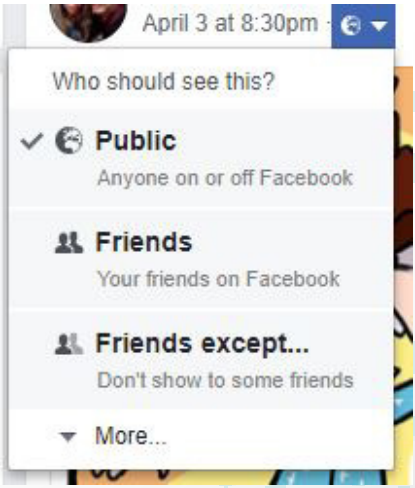


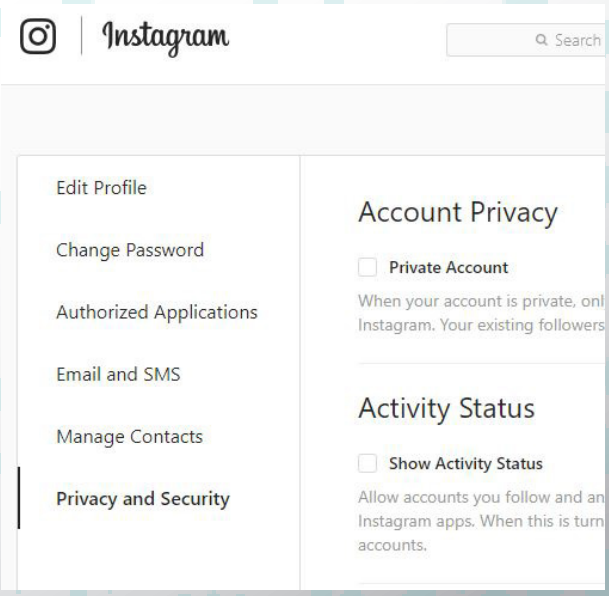
SOCIAL MEDIA

Social media has arguably become one of the most popular online activities this past decade - nearly every internet user regaularly utilizes some form of social media.
Not all social media platforms are alike, but most have certain aspects in common, which you should be aware of.

PRIVACY

1. You can often choose who sees your content: everybody or just your friends/ followers. Remember to read the website's help section if you're unsure of how to do so.



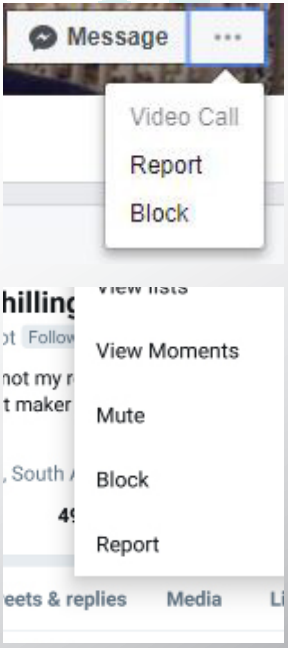


2. If you would like to know how social media websites use your data on their platforms, they have privacy policy documents as well as support pages. You can find them easily using a Google search.

3. Remember that any interactions on a public social media post (such as a business' page on Facebook) are visible to the public, and thus could potentially be seen by authorities, family or employers. Keep that in mind when you interact in this way.

HARASSMENT AND BULLYING

Bad, rude and/or unscrupulous people unfortunately are everywhere; the internet is no exception. Here are some tips to keep safe:



1. Major social media websites should have a "block" function, whereby you can prevent somebody from seeing or interacting with you.

2. You can also report somebody to the website's support team. They'll review your case and impose sanctions on the offending party if the situation calls for it.

3. Don't meet anybody you've met online unless it's in a public place and you're accompanied by a friend (if you have to meet them at all)

ANTIVIRUS AND ANTIMALWARE SOFTWARE

While being vigilant and maintaining your best judgement online will empower you to stay safe online, unfortunately there may be a situation where something gets through the cracks, such as unwanted software.

It's extremely important to have an antivirus and an antimalware programme installed on your device. Windows 10 (which, as of this writing, is what most new laptops and computers are equipped with) fortunately comes pre-installed with its own antivirus software. If you don't have one, Avast and AVG are two reliable ones. When looking around online for an antivirus solution, always look for reviews.

Antivirus software protects your device against viruses specifically, but unfortunately not malware. Malware is an umbrella term for all unwanted software, such as trojans, spyware, worms, adware and more. Therefore, you should also have an antimalware programme on your device. Malwarebytes is the most popular software for this purpose.

CONCLUSION

Now that you have reached the end of this handbook, you should have a solid foundation in empowering yourself to stay safe on the internet.

Before you go off to explore the vast world that is the intenet, just remember:

- You can always use Google (or Bing, or Yahoo!, or DuckDuckGo) to search for an answer to any question you may have, whether that question is about internet safety or anything else. Search engines are immensely empowering, as they function as a gateway to knowledge.
- Use your best judgement when deciding if you can trust a source of information on the web. You can ask for the opinion of a friend, colleague or family member if you are unsure. Not everything you read online is true!
- Remember to have fun!

THIS HANDBOOK WAS WRITTEN AND DESIGNED BY

JESSICA MICHAELS

FOR

WOMENSNET

WWW.WOMENSNET.ORG.ZA