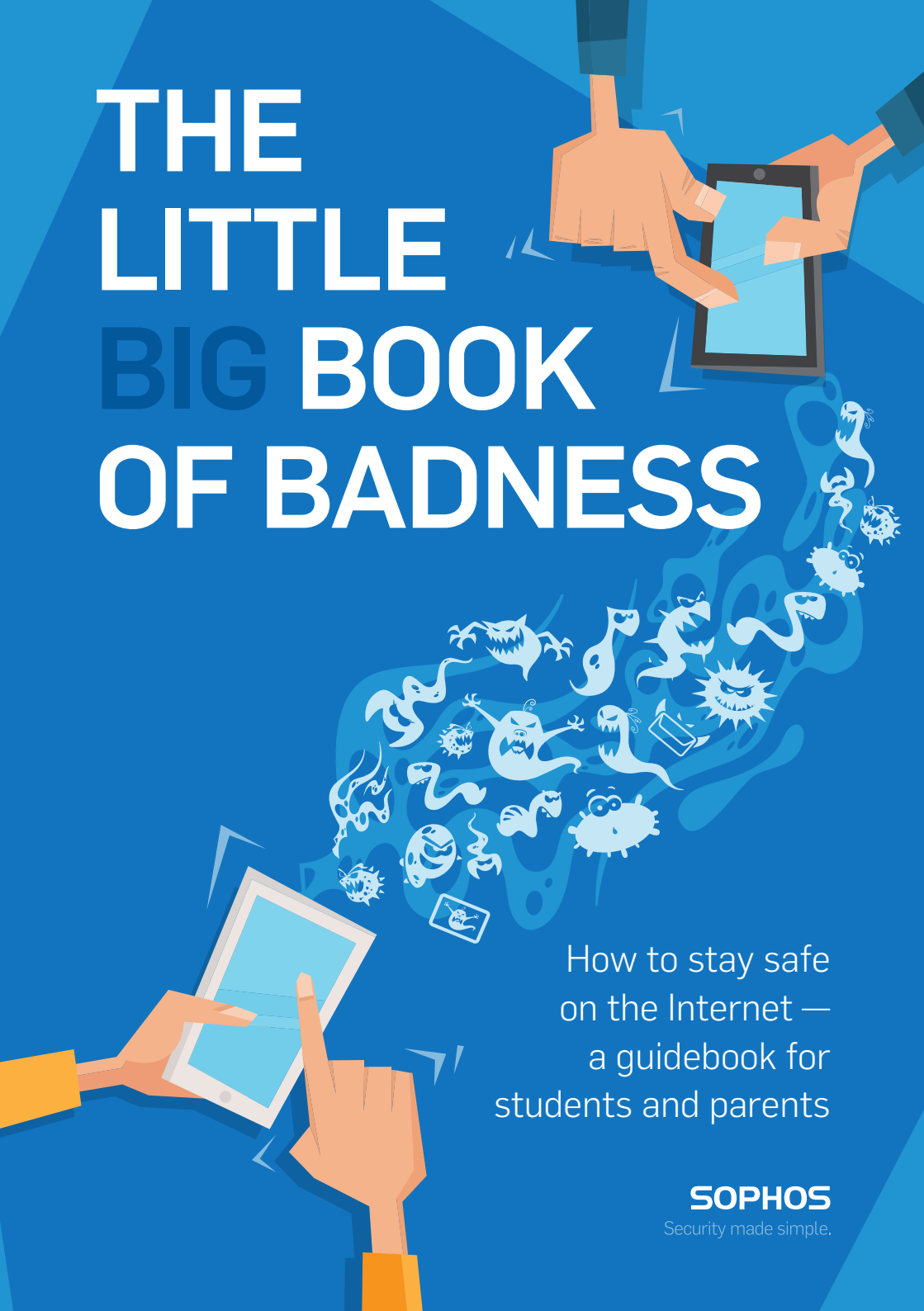
THE LITTLE BIG BOOK OF BADNESS



How to stay safe on the Internet — a guidebook for students and parents

SOPHOS
Security made simple.

USE THIS BOOK TO FIND OUT HOW YOU AND YOUR COMPUTER CAN STAY AWAY FROM BAD THINGS

CONTENTS

- Why you have to stay safe
- Don't be tricked
- Be careful
- Facebook
- Lock your phone
- Have loads of passwords
- Hard to guess passwords
- Don't leave things
- Don't remember
- Monsters and Penguins
- Watch out for WiFi
- Knock, knock. Who's there
- Happy app

WHY YOU HAVE TO STAY SAFE

The internet is amazing. It can lay the world at our feet. But just like the real world, not everyone has our best interests at heart. There are people out there who want to steal from you or do bad things to your computer, tablet or phone.

They want to pretend to be you so they can do crimes without the police knowing who they are (they'll think it's you!) They want to sell you things that don't exist or make you do things you don't want to.

They also want to take over your computer or phone and use it when you're not looking. Stay safe and follow the tips in this book to stop them!

DON'T BE TRICKED INTO GIVING AWAY PERSONAL DETAILS

Identity theft

When you answer emails, texts or phone calls make sure you keep who you are and where you live secret, unless you really know the person well.

Even if they just know your birthday or your pet's name, they might use these things to pretend to be you.

Keep your passwords safe. Anyone who has your password can go into your site or any of your online stuff and mess things up as a joke.

Stay on guard for these types of tricks to avoid falling for a scam, and tell your teacher or your parents or an adult you can trust.

BE CAREFUL USING COMPUTERS YOU DON'T KNOW

If you're using a computer in an Internet café or one that belongs to someone you don't know – be careful. They can have things like '**spyware**' on them. This takes your details secretly and passes it on to people who may cause you harm or upset.

This records what letters and numbers you have pressed on the keyboard (like passwords) and sends it to whoever set the keylogger up. Think carefully about the information you are sending on these public computers and try to avoid giving any really personal information when using devices that aren't your own.

They might have **viruses** too, so if you send a friend an email you could infect them – not friendly!

FACEBOOK NEEDS YOU TO BE 13 OR OVER

Facebook rules state that you should be 13 or more to have an account with them. The law doesn't allow them to have under 13s on their site.

If you have lied about your age, Facebook is unlikely to support you if things go wrong as you have broken their rules. If Facebook know that you are under-age they will close your account.

LOCK YOUR PHONE AND YOUR COMPUTER

If you have a phone or a computer of your own you should lock them when you're not using them.

They have lots of your special things on them. Private messages, photographs, homework, phone numbers, texts and other stuff you like. If you leave them unlocked anyone can see these things. They could delete them or steal them or just play tricks on you!

It only takes a second to lock them and then you know you're safe.

HAVE LOADS OF PASSWORDS

Passwords are a really easy and are a good way of staying safe but, you can't rely on just one. **Have a different one for everything** you do and you'll build a wall that keeps you and all of your stuff protected.

If you only have one and someone finds out what it is, they will be able to get into all of your sites, computers and phones.

You don't have to remember them all, you can store them in an **online password safe**. Then you just have to remember one.

MAKE YOUR PASSWORDS REALLY HARD TO GUESS

A hard to guess password will keep you even safer so **don't use obvious things**, like your dogs name or your Mum's name. Try using something that's about the site. If it's football you might use 'itsmyball'. And to make it even harder, you could change some letters to numbers – '1tsmyb4ll'.

See, it's easy to do but hard to guess!

See how many you can think of for all your sites.

DON'T LEAVE PERSONAL INFORMATION LYING AROUND

Data loss

Things with your name on or your address or your school or your mum's name could cause you problems.

If you leave them lying around people could pick them up and do bad things.

You could lose your school work from your computer or just lose your exercise books. If you're the clever one in class, everyone is going to want to copy your work, so put it away!

DON'T TICK 'REMEMBER PASSWORD' ON SITES

A lot of sites you visit will say "remember password for this site" – DON'T do it. If you do, the next person that uses your computer will go straight into your account.

Passwords are there to protect you, if you let the site, the browser or your computer remember it there's no point having it.

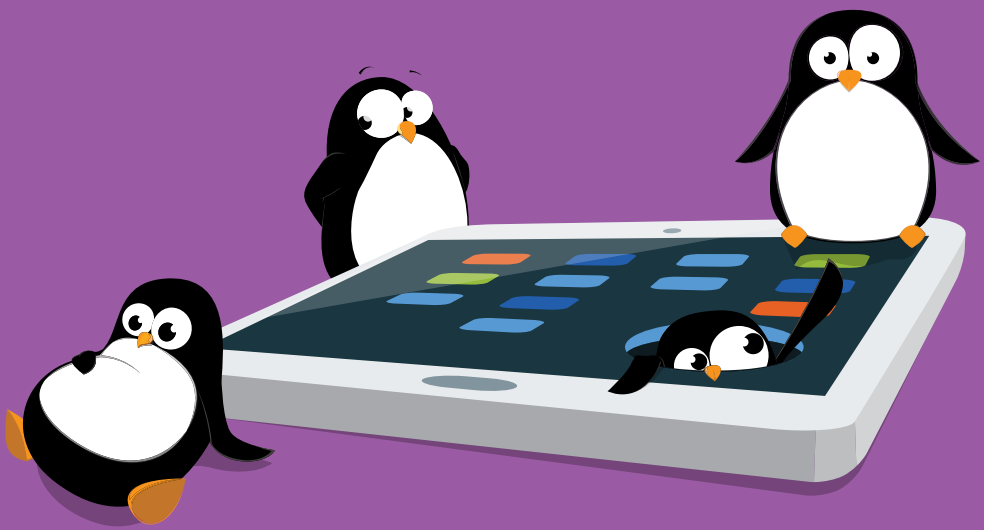
Use your brain to remember passwords or a good online password safe so you only have to remember one.

DON'T BE AFRAID OF 'SCAREWARE'

Sometimes a window will pop up on your computer saying that you have a virus and that you need to run a scan to get rid of it. This is Scareware. It tries to trick you by saying this so you click and download something. They will probably ask for money too.

It looks real and professional but inside it could be dangerous.

MONSTERS, PENGUINS, PETS AND PASSWORDS



There are lots of great, fun sites out there. Like Neo Pets, Moshi Monsters and Club Penguin. They're safe and easy to use but be careful with these too.

Don't give away details about yourself and don't share things like your birthday or where you live.

When you log on, and the site says "Remember password" don't click it because if you go away from your computer someone else could go straight into your account.

WATCH OUT FOR WiFi

Quick and easy-to-use, WiFi lets you do whatever you want while you're on the move. No wires or plugs, you're free to browse or play when you're out and about.

Make sure you are using a secure WiFi because if you're not people can tap into whatever you are doing or looking at. They could even hack into your device.

The WiFi you use should at least have a password.

KNOCK, KNOCK. WHO'S THERE?

New friends can be exciting but before you really get to know them it is important to still keep your private information safe. Remember it's difficult to always be sure that people online are who they say they are.

When you first meet people online it's always good to be careful.

MAKE SURE IT'S A HAPPY APP

Apps are great. Some are useful and some are just great to play. But some can harm your phone or device.

They're called 'rogue' apps and they look just like real apps but they can steal information, make your phone not work properly, make expensive phone calls without you knowing and lots of other bad things.

Make sure you only download apps from the real store and look for reviews. If LOTS of people like it with 5 stars it's probably OK.

IF IN DOUBT, SHOUT!

If you find anything you're not sure about tell your parents, teacher or an adult you can trust.

It's better to be safe than sorry!

SOPHOS

15.02.RP.bbb.simple