

# Cyber Security

{ Keeping the internet safe for you and your family



# The Five Things you MUST do

- ⌘ Learn the lay of the land
- ⌘ Protect your identity
- ⌘ Become a sceptic
- ⌘ Be aware of stranger danger
- ⌘ Be a good cyber citizen



# Learn the lay of the land

{ Understand the threats and what you can do to keep safe.



# The internet is everywhere...



# The next big thing... YOU





# Protect your identity

{ Your most valuable asset



# Your Identity, Your Asset

Definition: **Personal information** identifies you, your location or your financial assets.

- ⌘ Obvious: name, age, sex, picture, phone number, address
- ⌘ Less obvious: hobbies, interests, school mascot, gaming identities
- ⌘ Used for phishing scams



# The Top 20 Passwords

## THE TOP 20 PASSWORDS OF ALL TIME

1	123456	11	Nicole
2	12345	12	Daniel
3	123456789	13	babygirl
4	Password	14	monkey
5	iloveyou	15	Jessica
6	princess	16	Lovely
7	rockyou	17	michael
8	1234567	18	Ashley
9	12345678	19	654321
10	abc123	20	Qwerty

# More Password Facts

**4%**

Estimated percentage of consumers who use some variant of the word "password."

**25%**

Proportion of top 20 most commonly used passwords that are first names.

**16%**

Overall percentage of consumers who create passwords using a person's first name.

# Creating Secure Passwords

## CREATING A STRONG PASSWORD THAT IS EASY TO REMEMBER

### TIPS TO PASSWORD LENGTH AND SECURITY:

- Whenever possible, use at least 14 characters or more. The bare minimum is 8 characters.
- The greater the variety of characters in your password, the better.
- Use the entire keyboard, not just the characters you use or see most often.
- Test your password with a password checker.
- It is okay to write passwords down so they can be remembered.

### A SIMPLE TRICK:

- If you're concerned about being able to remember the code, here's a little memory-jogging trick: Take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m."

### HOW TO CREATE THE PERFECT PASSWORD

	WHAT TO DO	EXAMPLE
1	Start with a sentence or two, about 10 words total. <i>(Think of something meaningful to you.)</i>	<b>Long and complex passwords are safest. I keep mine secret.</b>
2	Using the first letter of every word, turn your sentences into an acronym.	<b>laccpasikms</b> <i>(10 characters)</i>
3	Add complexity. <i>(Make only the letters in the first half of the alphabet uppercase.)</i>	<b>LACpAsIKMs</b> <i>(10 characters)</i>
4	Add length with numbers. <i>(Put two numbers that are meaningful to you between the sentences.)</i>	<b>LACpAs56IKMs</b> <i>(12 characters)</i>
5	Add length with punctuation and/or symbols. <i>(Put a punctuation mark at the beginning and end.)</i>	<b>?LACpAs56IKMs"</b> <i>(14 characters)</i>

# What is Identity Theft

Unraveling the facts...

- ⌘ Identity thieves are clever, posing as friends, relatives and banks, to get people to reveal personal information. Watch for https and URL posers like paypa1. (Phishing)
- ⌘ Teens are just as likely as adults to become victims of identity theft -- when applying for a driver's license they may find one already has been issued using their name and Tax File Number, DL Number , Centrelink Customer Number etc..



# More Identity Tips

- Remember to share guidelines with your family:
- Do not share personal information such as your name, age, sex, picture, location/address, phone number, hobbies, interests, and tax file number, or bank account numbers.
- Create nicknames that do not reflect your own name or anything personal.



# Become a sceptic

{ Don't believe everything you read on the internet



# Pick the Fake...



You are our 1,000,000 Visitor!!!

 Like OMG! You just won a 1,000 dollar Walmart card! Don't worry, all we want is for you to click out annoying, seizure-making ad so we can destroy your computer with all our viruses and stuff and get your personal info!

Accept Ignore



# Phishing 101



- 1 **Generic greetings.**  
Many spoof emails begin with a general greeting, such as: "Dear PayPal member."
- 2 **A false sense of urgency.**  
Most spoof emails try to deceive you with the threat that your account is in jeopardy if you don't update it ASAP.
- 3 **Fake links.**  
The text in a link may attempt to look valid, then send you to a spoof address. Always check the source of a link before you click. Mouse over it and look at the URL in your browser or email status bar. If the link looks suspicious, don't click on it. Be aware that a fake link may even have the word "PayPal" in it.

# Spooftng 101


PayPal - Log In - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address [https://www.paypal.com/cgi-bin/webscr?cmd=\\_login-run](https://www.paypal.com/cgi-bin/webscr?cmd=_login-run)

**PayPal** Sign Up | Log In | Help

Welcome Send Money Request Money Merchant Tools Auction Tools

**Member Log In** Secure Log in 

Registered users log in here. Be sure to [protect your password](#).

Email Address:

Password:  [forget your password?](#)

New users [sign up here!](#) It only takes a minute.

Log In

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [User Agreement](#) | [Developers](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

[an eBay company](#)

Copyright © 1999-2004 PayPal. All rights reserved.  
[Information about FDIC pass-through insurance](#)

Notice the "https://..." but no padlock in the status bar!  
In fact, no status bar at all!

Bogus padlock here!

???

# More Phishing...



Dear ANZ BANK customer,

We recently reviewed your account, and suspect that your ANZ BANK account may have been accessed by an unauthorized third party. Protecting the security of your account and of the ANZ BANK network is our primary concern.

Therefore, as a preventative measure, we have temporarily limited access to sensitive ANZ BANK account features.

Click the link below in order to regain access to your account:

<https://www.anz.com/account/update.asp>

For more information about how to protect your account, please visit ANZ BANK Security Center.

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire ANZ BANK system.

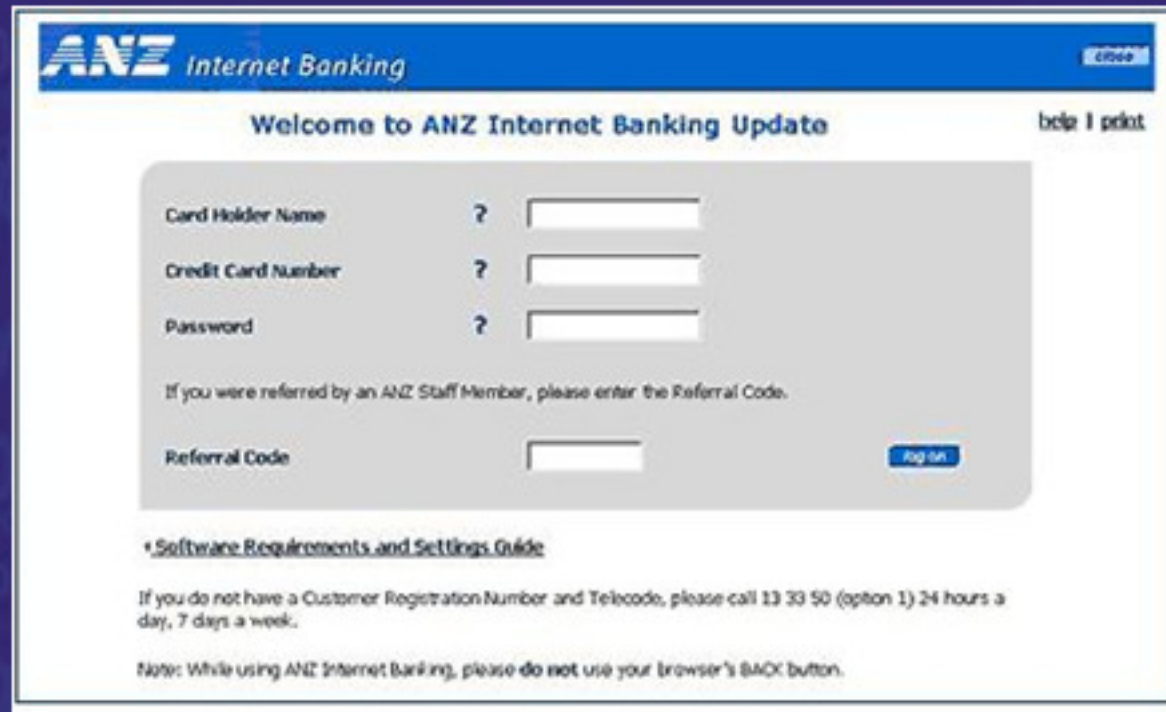
Thank you for your prompt attention to this matter.

Sincerely,

The ANZ BANK Security Department Team.



# And spoofing...



The image shows a screenshot of the ANZ Internet Banking Update login page. The page has a blue header with the ANZ logo and the text "Internet Banking" and a "close" button. Below the header, it says "Welcome to ANZ Internet Banking Update" and "help | print". The main content area is a light gray box containing the following fields:

- Card Holder Name ?
- Credit Card Number ?
- Password ?

Below these fields, there is a note: "If you were referred by an ANZ Staff Member, please enter the Referral Code." and a "Referral Code" field with an "agree" button.

\*Software Requirements and Settings Guide

If you do not have a Customer Registration Number and Telecode, please call 13 33 50 (option 1) 24 hours a day, 7 days a week.

Note: While using ANZ Internet Banking, please do not use your browser's BACK button.

# Top 10 Scams...



## Job Hunter Scams

**Pitch:** We will match you up with a perfect job that's ready and waiting for you.  
**Target:** Bank account and/or Social Security numbers.  
**Result:** Victims must pay a fee to be considered for a job. Out of money they don't have, still no job.



## Debt Relief and Settlement Services

**Pitch:** We will help you eliminate most or all of your debt (for a fraction of the amount you owe).  
**Target:** Collection of upfront fee(s) in order to "settle your debts."  
**Result:** Potentially leave the consumer drowning in even more debt than they started with and completely run their credit.



## Work from Home Schemes

**Pitch:** Fire your boss! We can teach you the secrets to making money online, assembling items at home or being a mystery shopper.  
**Target:** Employees tired of the same 9-5 routine. In some cases, they unknowingly work to fence stolen goods.  
**Result:** Instead of getting paid, you can end up losing hundreds—if not thousands—of dollars or in legal trouble.



## Timeshare Resellers

**Pitch:** We will help you get out from under your costly vacation property and do it fast.  
**Target:** Collect several thousand dollars to cover fees.  
**Result:** After paying the fees, the seller never hears from the company again.



## Not So "Free" Trial Offers

**Pitch:** Try a free offer and never be charged - unless you want to continue the offer.  
**Target:** Repeated monthly billings.  
**Result:** The free trial offers seem easy, the consumer is repeatedly billed every month and is difficult to cancel.



## Rogue Home Repair/Roofers

**Pitch:** We can get that tree out with half down, and fix your roof for a fraction of what that guy is going to charge you.  
**Target:** Initial upfront fee(s) to get the job started.  
**Result:** Homeowners are often stuck with either an unfinished or never started project and are out the initial money as well.



## Lottery and Sweepstakes Scams

**Pitch:** You have won a large lottery or sweepstakes and just have to cover taxes before receiving your money.  
**Target:** Payment under the guise of "covering taxes" or other bogus "fees."  
**Result:** The victim wires the money, but the prize or money never arrives.



## Advance-Fee Loan Scams

**Pitch:** You or your business qualifies for a large loan but you must pay some upfront fees.  
**Target:** Initial upfront fee(s) - often more than a thousand dollars.  
**Result:** The victim wires "the fee" to the scammers but never receives the loan.



## Over-Payment Scams

**Pitch:** Oops, I accidentally sent you too much money, would you please wire some back?  
**Target:** Any amount of money that is wired back.  
**Result:** Transaction is reversed, and the victim is out the money wired back to the scammers.



## Identity Theft

**Pitch:** Hi, this is a very legitimate business, we need to confirm some information today, is that ok?  
**Target:** Gathering personal sensitive information to open lines of credit or just straight stealing money from the victim's account.  
**Result:** Victim is left spending countless hours trying to repair all of the damage the thieves have done or are still doing.



# If in doubt, check it out

⌘ Remember if it sounds too good to be true...IT IS!

⌘ Resources:

- ⌘ Urban Legends Debunked [snopes.com](http://snopes.com)
- ⌘ SCAMS uncovered: [scamnet.wa.gov.au](http://scamnet.wa.gov.au)
- ⌘ Financial Scams [moneysmart.gov.au](http://moneysmart.gov.au)



# Stranger Danger

{ In a digital world, where everyone is a stranger





*"On the Internet, nobody knows you're a dog."*

# What is a Cyber Predator

- ⌘ Definition: A Cyber predator uses the Internet to hunt for victims to take advantage of in ANY way, including sexually, emotionally, psychologically or financially
- ⌘ Cyber predators know how to manipulate kids, creating trust and friendship where none should exist



PhotoshopTalent.com



# How “findable” are you?

The image shows a screenshot of a Facebook page for a "Senior High School". The page has a cover photo of a school building and a profile picture that is redacted with a black box. The page type is "School".

On the left sidebar, there are navigation options: Info, Friend Activity, Related Posts (highlighted), and Wikipedia. Below these, the number "1,599" is circled in red, with the text "like this" underneath. Below that, it says "20 are talking about this". At the bottom of the sidebar are links for "Create a Page", "Add to My Page's Favorites", and "Report Page".

The main content area shows "Related Posts". The first post is by "Naimur Rahman Mahir" with the text "my lil sis reads here..hmm...quite beautiful...!". The second post is by "Denean" with a profile picture circled in red and the text "That looks more like a shit hole this is cali baby lynwood high class of 92 is surely not a shit hole like you try to call stay your white washed ass in canada and don't try to step up and be hard on someone you don't even know". The third post is by "Josh" with the text "You tell em sister no one comes up into my house WEST SIDE YE".

At the bottom, there is a comment by "Liam Smith" that says "willo blowws".



CAPEL



# Quick, easy & dangerous!

The image is a collage of several screenshots illustrating a location-based marketing strategy. At the top left, a Facebook profile for 'Meg' is shown, with a red circle highlighting a photo of two young women. Below this is a 'White Pages' advertisement with the text 'It's how we connect' and 'hi hi hi'. The middle section shows a Google search for '3 orbison st willetton', with a 'Business' tab selected. Below the search results, a Google Street View image of a residential property is displayed, with a red location pin and a 'Directions' button. The address is partially obscured by a black box, but the location is identified as 'Western Australia, Australia'. The bottom right corner of the collage features the 'rethink MARKETING' logo.

# Identifying a Predator

Unraveling the facts...

⌘ What children need to look out for is **not** a certain stereotype of a dangerous person but certain types of behavior...

⌘ Excessive Praise

⌘ Questions about what they're wearing or what they're doing ?

⌘ Questions designed to determine whether their parents are nearby including where's the computer in the house



# Reporting the problem

- If you suspect that you are being stalked or the victim of inappropriate communication, report it to a trusted adult and/or to Crime Stoppers.
  - ✓ <http://crimestoppers.com.au/>
  - ✓ 1-800-333-000

# Cyber Bullying

{ And other things to think about as a good cyber citizen



# What is Cyber Bullying



Cyberbullying occurs when a child or teenager is tormented or harassed by another child or teen using the Internet or mobile phones. In order to be considered cyberbullying, both parties must be minors. If the harasser is found to be an adult, it is considered cyber harassment, a much more serious offense.

## TYPES OF CYBERBULLYING

There are several distinct types of cyberbullying that school workers and parents need to be aware of. Each type involves a different kind of bully, different motives, or the use of various technology. Once school officials, parents, and law enforcement officers know which types of bullying are carried out, they determine appropriate disciplinary action, and work to prevent similar incidents from occurring in the future.

### FLAMING

An intense, angry argument carried out over instant messaging, social networks, or chat rooms.

### HARASSMENT

Embarrassing, hurtful, or terrorizing messages aimed directly at an individual or group using text message or online communication.

### ANONYMITY

Any form of harassment or threats issued by an anonymous bully. The harasser may use an online alias (also known as a screen name), a blocked phone number, or a borrowed cell phone to bully, making it difficult to determine their identity.

### MASQUERADING

Masquerading occurs when a cyber bully goes to great lengths to make themselves appear to be someone they are not. For example, a cyber bully may set up a Facebook profile under another student's name and use it to harass people.

### OUTING

A public showing of personal conversations. Outing occurs when the harasser prints or displays email, text, or chat communication that the victim intended to be kept private.



Little help here...



# 4 Types of Cyber Bullies



stopcyberbullying.org

**THE  
VENGEFUL  
ANGEL**



stopcyberbullying.org

**"POWER-  
HUNGRY" AND  
"REVENGE OF  
THE NERDS"**



stopcyberbullying.org

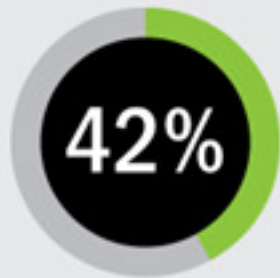
**"MEAN  
GIRLS"**



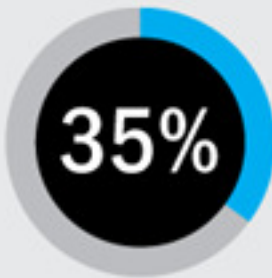
stopcyberbullying.org

**THE  
INADVERTENT  
CYBERBULLY**

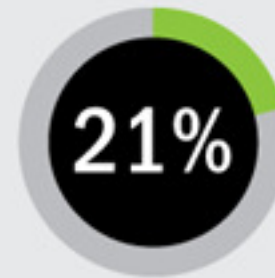
# Who gets Bullied?



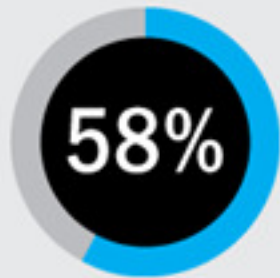
42% of kids have been bullied while online. 1 in 4 have had it happen more than once.



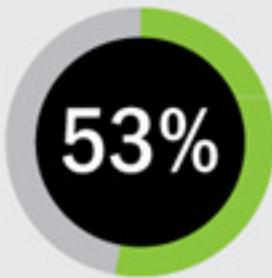
35% of kids have been threatened online. Nearly 1 in 5 have had it happen more than once.



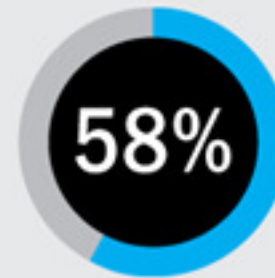
21% of kids have received mean or threatening e-mail or other messages.



58% of kids admit someone has said mean or hurtful things to them online. More than 4 out of 10 say it has happened more than once.



53% of kids admit having said something mean or hurtful to another person online. More than 1 in 3 have done it more than once.



58% have not told their parents or an adult about something mean or hurtful that happened to them online.

Additionally, a 2010 report compiled by the Cyberbullying Research Center looked at cyberbullying behavior among middle school children. The Center discovered that:



30% of middle school students were victims of at least one of nine forms of cyberbullying two or more times in the past 30 days.



22% of middle school students admitted to engaging in at least one of five forms of cyberbullying two or more times in the past 30 days.

# What we can do...



Never share information about your children's online activities with other parents or children, including gaming names or username/passwords, as they could be used against them.



Teach your children not to respond to cyberbullying attacks. Contributing to the conversation often escalates the harassment.



Download and save all abusive messages to report to school officials and, if necessary, law enforcement authorities.



Contact your Internet service provider to report code of conduct violations and seek action against the bully.



Use filtering and blocking software as a part of a comprehensive approach to online safety, but understand software programs alone will not keep safe or prevent cyberbullying.



Model appropriate technology usage. Don't harass or joke about others while online, especially around your children. Your kids are watching and learning.



Cultivate and maintain an open, candid line of communication with your children, so that they are ready and willing to come to you whenever they experience cyberbullying.



Encourage your child to report the bullying activity and discuss the experience with you or a school counselor. It is a myth that "weaklings tattle."

# Cyber Citizenship

{ How to be a good citizen online



# The Dos...

- ⌘ **DO** use the Internet to help with schoolwork.
- ⌘ **DO** use the Internet to "visit" museums in far away places
- ⌘ **DO** be careful about talking to "strangers" on a computer network
- ⌘ **DO** respect the privacy of other users on the Internet
- ⌘ **DO** be careful when you "download" (copy) programs from the Internet



# And the Don't's

- ⌘ **DON'T** give your password to anyone
- ⌘ **DON'T** answer messages that make you feel uncomfortable because they seem improper, indecent, or threatening
- ⌘ **DON'T** give any personal information, such as your family's address, phone number, credit card
- ⌘ **DON'T** arrange to meet anyone you've met on the Internet without telling your parents
- ⌘ **DON'T** try to hack into computers
- ⌘ **DON'T** steal copyrighted programs, books, magazines, movies or music.
- ⌘ **DON'T** view, copy or share pornography
- ⌘ **DON'T** copy material that you find on the Internet and pretend that it's your own work.



# Top Tips for Parents

- ⌘ **Keep your computer in a central and open location**
- ⌘ **Use the Internet with your children**
- ⌘ **Implement parental control tools**
- ⌘ **Consider partitioning your computer into separate accounts**
- ⌘ **Know who your children's online friends are and supervise their chat areas**
- ⌘ **Teach your children never to give out personal information**
- ⌘ **Know who to contact if you believe your child is in danger**
- ⌘ **Have a digital lights out policy – switch it off at night.**



# What we have covered

- ⌘ Learn the lay of the land
- ⌘ Protect your identity
- ⌘ Become a sceptic
- ⌘ Be aware of stranger danger
- ⌘ Be a good cyber citizen



Where you can find out more...

cyber(smart:)

[www.cybersmart.gov.au](http://www.cybersmart.gov.au)

