DANGER DETECTIVE

Phishing Emails

1. **Trust your instinct**
   If it doesn't make sense, or is too good to be true
2. **Check the 'from' address**
   Tap or click on the email address that sent the email
3. **Check for spelling errors**
   Grammar matters, typos or weird language use
4. **Question actions needed**
   Be wary about downloading or updating account details
5. **Be a vigilante**
   Google 'phishing [company name]' eg 'phishing Apple' to find where to forward the email to

Facebook Fakes

1. **Check the profile pic**
   You can image search the pic on Google to check validity
2. **Check the bio for real-ness**
   Is this person from Sydney, works at Sydney Hospital, attended Sydney High
3. **Search Facebook for name**
   See if any profiles with the same name and profile pic appear
4. **Do I know you?**
   Have you met them in real life?
5. **Don't share personal info**
   Close friends or family accounts may have been 'copied'. If they ask for personal info, call them!

Real Websites

1. **Check the www address**
   Use your common sense!
   eg www.f7834j5hsd.com – fake
2. **Check for SSL certificate**
   The green lock or padlock represents approved websites for banking / finances
3. **Don't be fooled by looks**
   It is easy for a clever coder to recreate a known website
4. **Do a Google search**
   Google the company name and check out these websites
5. **Still don't fill**
   Only fill out your info when you are sure it is real

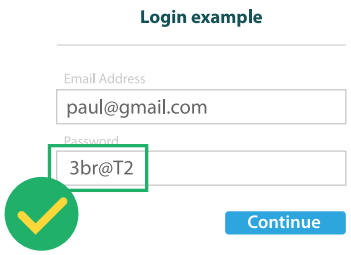
Notes

www.dotjess.com/danger

Be Connected

Passwords

Here are some top tips for creating a strong password, one that can't be guessed by other people.



Why we need passwords

Many websites will ask for personal details, such as your name, address, date of birth or credit card information. To protect that information, you have to create a password. Creating a good password that can't easily be guessed is an important way of protecting yourself online.

Why good passwords matter

If somebody else gets hold of your password, they can use that password to access the personal accounts on the websites you've visited. That means that your email, banking, shopping and social media accounts might be hijacked. A good password makes it much harder for someone to guess your password, which means that your personal accounts can be far more secure.

What not to do

Create a secure password

There are some common mistakes that people make when creating passwords. These include:

- Using obvious or very simple passwords, such as **1234** or **password**.
- Using personal information, like birthdays, or the names of pets or family members.
- Using dictionary words, such as January, beach or family.
- Using the same password for multiple websites.

You should avoid making these mistakes yourself. Instead, you should create what's known as a 'good' password, one that can't be easily guessed.

How to create a good password

Don't use dictionary words

A good password looks like it's just a jumble of letters, numbers and symbols. For example, **3br@T2** or **Figit32!** are good passwords.

But remembering those types of passwords can be hard, so there are some tricks you can use to create good passwords that you can remember.

- You can use the substitution method. This is where you take a word and replace several letters with numbers, symbols and upper case letters. For example, **friday** could become **f7!Day**.
- You can use a phrase or lyric that you remember and make the password from the first letter of each word. For example, **Married on the 24th of July** could be used to remember the good password, **Mot24oJ**.

Storing passwords in a web browser

Over time, you'll need to remember a lot of passwords. Your web browser can help with that. Just follow these steps:

1. When you enter the password on a website, your browser will ask if it you would like it to remember the password.
2. Only click **Yes** if you own the computer. If you're on a public computer, click **No** or **Never**.
3. If you clicked **Yes**, the next time you visit that website, the password will be filled in for you.

Your browser can help with password management

Keeping it up

You should create a new good password every time you're asked to create a new password. As an added precaution, you can change your most important passwords every few months.

Sign up for more free lessons online now:
Go to www.dotjess.com/learn
Click on BeConnected Sign Up (green border, white button with green writing)
Fill in your details and select DotJess as your support centre
Click Sign Up For Free and access the topic library.