This Leaflet is a Short Guide to:

Keeping passwords safe

Stoping the infection and spread of malware

Network privacy and securety

Keeping your information in the right hands

I wrote this guide as part of my BTEC software development course. The objective of the task was to inform users about internet security, making them aware of the dangers that come with using technology, and how to effectively fix problems, or better yet, avoid them all together.

The content of this document was written by

Tyler Smith

Under the GPLv3

Images from http://uscollegesearch.org

technology
secure

secure IT

Your guide to keeping safe with technolgy

technology
secure

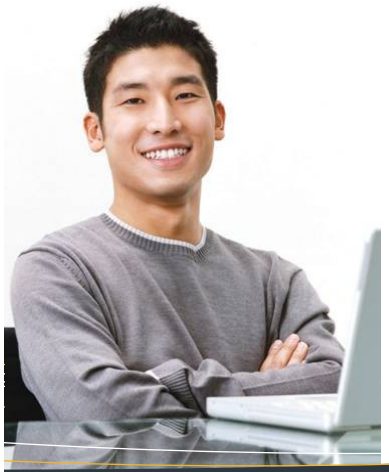
Ways to keep you safe with technology

A FEW SIMPLE STEPS TO KEEP YOUR PRIVATE INFORMATION OUT OF THE WRONG HANDS.

Follow these simple steps, and your experience is sure to be smooth and problemless. Remeber, privacy isn't about anonimity, it's about drawing the line between gathering information, and invading your freedom to do as you please

THINGS TO REMEMBER:

- DATA SENT IS OUT OF YOUR CONTROL
- ONLY DOWNLOAD TRUSTED SOFTWARE
- KEEP SOFTWARE UPTO DATE
-



Firewalls:

There are external and internal firewalls. The external firewall decides the flow of network ports to the devices within the network. Internal firewalls prevent applications from opening nd using particular ports. This helps network security as it means that even if a program is vulnerable to attack, it is only visible from the local network.

Access Control Methods

These are systems put in place to restrict users from accessing certain areas of a system. This is useful for keeping the system maintained, and prevents the distribution of malicious software on the network. On a system with a user group system, such as a linux workstation system, it only requires you to modify the permissions to a file or folder to restrict different permissions such as read, write, and execute permissions. This keeps the system safe from the users downloading viruses, and edit documents that they shouldn't, etc.

Secure Payment Systems

It is important to make sure that any payment systems you use online are secure. You can check by using an up to date browser, and looking on the left of the address bar. If a padlock is shown, the connection is secure. Web connections are usually done over SSL. An SSL tunnel is created by encrypting your HTTP requests (along with your public key) using SSL certificates as a public key, and then when the server decrypt the information, they encrypt your response with your public key. This type of low maintainence encryption is called transparent encryption. This protocal is labeled 'HTTPS' and helps keep customer data private.

Disaster Recovery

Disaster recovery is a procedure put in place to make sure that data is kept safe. The procedures can include keeping backups on harddrives kept offsite, sometimes outsourcing it to external companies servers. This way, even if a natural disaster strikes, or data is corrupt, a second copy of the data is accessable.

Complicated Passwords

Useing passwords with capital letters, numbers, and symbols are 4 times harder to crack, and take literelly years longer.

Click Confidently

Every webpage you visit, every program you download has the potential to get full access to your machine. Do you really trust the link you're clicking?

Update Regularly

The most common feature of updates is to keep up with security. Applications such as Skype, Chromium, and even your anti-virus, have the potential to leak to attackers. Luckily, there's a team of people working to help you, all you need to do in press update.

COMPUTERS ARE HACKED, AND PERSONAL INFORMATION IS LEAKED EVERY DAY. WILL THE NEXT ONE CONTAIN YOURS?

Your profile of information is very useful to marketing campaigns, but is also a killer tool for internet hackers. Your email address will go for hundreds of pounds in large databases along with thousands of other innocent internet users to be used for mass spam attacks, attempting to steal more sensitive information such as credit card details.