Increasing Online Security

UBS Brasil CCTVM's goal is to provide quality products and services to its clients, and in order to do so, it searches for the newest technology developments available in order to update its data security systems in order to protect its client's personal data. However, UBS Brasil CCTVM recognizes that the widespread use of the internet and of electronic communication systems might present security and data protection risks to the average user.

Aware of such risks we have prepared a short guideline with some security practices and tips that may help our clients with improving their overall online navigation and internet use security.

1. Always keep your software up to date.
Not all software scripts are exempt of failure, and for that reason their developers are constantly releasing software patches and updates in order to correct bugs and breakdowns detected from time to time. One effective way to protect yourself is to download the newest version available of your software - specially the new patches for your operating system and web browser.

Some programs are already set to automatically check for updates – if not, it is generally possible to turn on automatic updates in the settings of most software. Also, most operating systems and browsers have their own security and privacy setups, which can be explored and adjusted on their menus – usually these will be available on the upper left bars in the "Options", or "Tools" tabs, depending on the software used.

2. Make sure you have security software installed on your personal computer.
It is of extreme importance that your computer is secure: make sure you have anti-virus software installed and that your firewall is enabled and updated. You may also install other security software, e.g. backup and anti-malware programs.

The anti-virus software helps tracing viruses that can steal data, thus we strongly recommend to keep it updated and to scan your computer periodically. If you find any infected file, you should evaluate if it is worth repairing or if you should delete it. Firewall programs are set to block the communication and access of external and non-authorized parties to your computer, protecting your data from hackers.

3. Create and use your password in the safest way.
Alongside general security tips (e.g. avoid sharing your personal passwords with others and avoid using easy passwords such as birth dates and phone numbers), we suggest that your passwords are created with several characters (at least eight characters long) and contain a mix of case letters, numbers and symbols.

Do not forget to change your passwords regularly and do not write them down or store them in papers and files that might be exposed. When navigating in the internet, it is also recommend to confirm if the website you are currently in might be caching your data (e.g. fill-in forms), and if you are navigating in a secure connection, also avoid logging into your internet banking if navigating in a unsecure connection or in public computer.

4. Be aware of links and attachments to your e-mail and take security measures when installing software and apps.
E-mail spams besides being bothersome might include attachments, links or images that might be concealing malicious software created to steal information. This dynamic is normally triggered when user clicks on the links to the attachment or files. For that reason we recommend user not to open attachments or links unless he is aware of the origin of the message and of its content. Even when receiving messages from known emitters it is also recommended to confirm the authenticity of the message before opening the files as a known user may have been infected by programs

triggered to send infected messages to all address databases.

Spam messages are often depicted as offers, pictures and articles that arouse general user curiosity with media appealing content. These messages might contain programs developed to steal your personal data. Caution is always advised when handling unknown messages. Other common frauds are deployed through fake websites, including social networks; these are tailed and programed in a way that they are able to steal user data and passwords. Therefore we recommend an increased level of caution when handling unknown attachments and file extensions.

Other known methods used in internet fraud are by means of the creation of fake websites, and social network pages that are able to capture user personal information and passwords. Common approaches include sending: fake billing requests, messages from credit bureaus, online greeting cards, gift certificates, prize awards, communication from government authorities and tax authorities, online banking links, amongst others.

More sophisticated scams are also being used in the internet. Of these scams it is important to mention "phishing scams", this kind of fraud is widespread and is used to steal financial information. In order to avoid being caught in this kind of scam it is advised not to answer e-mails from unknown emitters and from financial institutions as these will not request user information via e-mail. Should there be any doubt concerning the origin of the message it is recommended that user check with the emitter the authenticity of the message.

Viruses and malicious programs may be hidden in apparently harmless software and applications. Therefore, it is recommended that user only download software in confirmed and known websites, and to avoid installing software which's use is unknown to the user. Scroll bars and file sharing programs are some examples of software that are known for hiding malicious files, so always check their origin before downloading.

5. Precautions and safety tips when discarding your Personal Computer.

With the vast array of technological improvements available users have been changing there computers more constantly. It is advised to check the data stored in the personal computer before deciding to discard it. Please note that discarding a computer inappropriately may bring risk and harm to user if his personal files are still available in the computer data files. Therefore computer should only be discarded after its memory is completely erased because it may contain portions of data stored in its residual memory, including passwords, account numbers, license keys, addresses, telephone numbers, and other such data, that may be attractive for social engineers and data thieves.
In order to prevent these risks and to improve discarding procedures the installation and usage of memory deleting programs is recommended, user may additionally opt to make a backup of his data in order to preserve his information.