Tutorial ICT

Bersama FIRKHAN
firkhan.uthm@yahoo.com

Panduan keselamatan digital di pejabat

PENGGUNAAN komputer di pejabat sudah menjadi kelaziman bagi sesebuah syarikat bagi memudahkan pekerja menyelesaikan tugasan kerja. Namun begitu, tanpa disedari penggunaan komputer yang tidak selamat dan tidak betul boleh mengundang masalah keselamatan digital kepada satu komputer atau keseluruhan prasarana digital bagi organisasi tersebut.

Berikut dibincangkan beberapa perkara yang boleh diambil bagi menjaga keselamatan digital bagi sesebuah pejabat.

1 Pastikan diwujudkan polisi keselamatan digital bagi penggunaan prasarana digital di pejabat yang merangkumi sepenuhnya aspek penggunaan digital kini seperti pekerja dari rumah, penggunaan peralatan digital kepunyaan peribadi, capaian perkhidmatan digital organisasi dari tempat lain dan sebagainya. Pemahaman dan pematuhan para pekerja terhadap polisi keselamatan digital ini sangat penting bagi keberkesanan perlaksanaannya.

2 Pastikan semua sistem maklumat dan aplikasi komputer dikemas kini dengan tampalan terkini terutama bagi sistem pengoperasian dan aplikasi keselamatan seperti perisian antivirus.

3 Pembersihan memori *cache* bagi komputer yang digunakan. Kelebihan pembersihan memori cache ini dapat mengelak daripada *malware* bersembunyi di dalamnya dan dapat capaian laman web dengan versi terkini.

4 Pembersihan memori *cookies* bagi pelayar web yang digunakan bagi penjagaan keselamatan maklumat peribadi. Boleh dibersihkan secara berpilih atau sepenuhnya.

5 Penggunaan kata laluan yang kental dan pengesahan dua faktor. Kata laluan yang kental boleh dibina dengan menggunakan kaedah *passphrase* atau kelulusan frasa yang panjang.

6 Semak keselamatan penggunaan penghala atau *router* di pejabat. Laksanakan kekerapan pertukaran kata laluan bagi penghala tersebut.

7 Pastikan masuk atau berada ke dalam rangkaian komputer yang betul terutama ketika capai prasarana digital syarikat menggunakan rangkaian nil wayar daripada rumah atau rangkaian awam. Jangan sesekali menggunakan rangkaian nil wayar awam dalam melakukan kerja terutama mencapai perkhidmatan VPN (*Virtual Private Network*) syarikat.