KEMBARAN A KEPADA
BSPP(DPI-CPS).100-11/1/1
BERTARIKH 30 OGOS 16

TATACARA PENGGUNAAN DAN PENGURUSAN E-MEL

Bil	Perkara	Penerangan
(a)	(b)	(c)
1.	Menyulitkan atau menetapkan kata laluan (*password*) bagi fail kepilan (*attachment*) yang dihantar.	Ini bertujuan untuk melindungi dokumen yang dihantar bagi menjamin keselamatan dan kebocoran maklumat. Untuk memperketatkan lagi keselamatan, pengguna dinasihatkan memaklumkan kata laluan kepada penerima menggunakan medium lain contohnya menggunakan aplikasi Telegram.
2.	Menggunakan kata laluan berbeza bagi setiap fail kepilan yang dihantar.	Menggunakan kata laluan yang kukuh sekurang-kurangnya lapan aksara dengan kombinasi huruf, nombor atau aksara khas bagi memperketatkan keselamatan. Contoh: M@lays1A2016. Pengguna dinasihatkan tidak menggunakan kata laluan yang sama bagi akaun e-mel dan fail kepilan. Ini akan memudahkan penyerang untuk meneka kata laluan tersebut.
3.	Mengenal pasti identiti pengguna.	Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel. Ini bertujuan untuk melindungi maklumat ATM daripada sebarang bentuk penyalahgunaan Adalah dinasihatkan supaya tidak membuka sebarang fail kepilan daripada penghantar yang tidak dikenali atau penghantar yang dikenali namun pengguna tidak menjangkakan e-mel tersebut. Perkara ini akan memudahkan penyerang untuk menghantar e-mel yang kelihatan daripada rakan tempat kerja atau rakan di dalam organisasi.
4.	Pengguna hendaklah mengelak membuka fail kepilan e-mel daripada penghantar yang tidak diketahui dan diragui.	Objektif penyerang adalah untuk menyebarkan *malware code* bagi menjangkiti dan mengawal peranti pengguna. Selain dari memberikan pautan, penyerang akan menghantar e-mel beserta fail kepilan seperti dokumen *Word.* Membuka fail kepilan tanpa mengetahui tujuan dan isi kandungan emel fail tersebut dan ia akan memberi peluang kepada penyerang untuk menjalankan aktiviti tidak dingini seperti *phishing, spamming,* ancaman virus dan lain-lain *malware.*

Bil	Perkara	Penerangan
(a)	(b)	(c)
5.	Pengguna adalah bertanggungjawab untuk melaporkan kepada mafcert@siberoc.mil.my apabila menerima e-mel yang meragukan atau tidak dikenali.	Jika pengguna mengesyaki e-mel yang diterima adalah meragukan, pengguna hendaklah segera memaklumkan kepada mafcert@siberoc.mil.my. Pengguna juga dinasihatkan supaya *forward* e-mel tersebut kepada mafcert@siberoc.mil.my sebelum memadamnya (*delete*).

NOTA:

1. Untuk pemeriksaan lanjut, jika pengguna merasakan pernah membuka fail kepilan dalam format Word bertajuk 'attachment.doc', pengguna boleh ke *path* berikut untuk memeriksa sama ada terdapat fail bernama 'doccache.db' diwujudkan: **C:\users\<username>\AppData\Local\doccache.db.**

2. Fail ini adalah tersembunyi (*hidden file*), pengguna perlu menetapkan *show hidden files* pada tetapan.

3. Sila hubungi Bahagian ini dengan segera jika terdapat fail doccache.db tersebut.

4. Pengguna masih boleh meneruskan kerja harian menggunakan komputer.