Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Security News of the Week

by Thomas Martin, Manchester Metropolitan University, Senior Lecturer

Monday 14th December 2020

Subway sandwich scam mystifies loyalty card users

Several Subway customers have reported receiving phishing emails. The links point to a macro spreadsheet that tries to convince the victim to disable the security protections. It is not clear how the phishers got the names and email addresses, as they seem to be targeted specifically at Subway customers. Users are encouraged to ignore documents that insist on changes to security settings. Read more>

US treasury and commerce departments targeted in cyber-attack

The US Cybersecurity and Infrastructure Security Agency (CISA) has announced that the Treasury and Commerce departments have been hacked. The attack appears to have been executed through the injection of malicious code into updates for the SolarWinds network monitoring tool. The level of expertise required for such an attack is believed to require the resources of a nation state, with rumours circulating that it was Russia who was behind the attack. Read more>

US telcos ordered to 'rip and replace' Huawei components

The United States are taking further steps to distance themselves from Huawei. The Federal Communications Commission (FCC) has ordered companies to remove Huawei equipment from their networks, with subsidies provided for their replacement. The US Administration has accused Huawei of being a threat to national security due to their close ties to the Chinese military and intelligence communities. Huawei have denied the accusations that the Chinese government has inappropriate influence over their operations but are still facing increasing difficulty in obtaining and holding onto contracts with other countries around the world. Read more>

Ex-Cisco engineer who nuked 16k WebEx accounts goes to prison

A former Cisco employee was sentenced to two years in prison and fined $15,000 for sabotaging the company's systems after his departure. He deleted 456 virtual machines which led to the shutting down of more than 16,000 WebEx accounts. The damage took two weeks to repair and Cisco had to refund $2.4 million to customers. The ex-employee was found guilty of Intentionally Access a Protected Computer Without Authorization and Recklessly Causing Damage and will being serving his sentence on February 10, 2021. Read more >