520.743.7554
info@computerdimensions.net
www.computerdimensions.net

A couple of topics on the agenda today.

**Topic 1: Windows 10 will become an automatic 'Recommended' update next year**

Ever since Microsoft launched Windows 10, the company has come under fire for controversial update and deployment policies. Microsoft has been caught deploying a 6GB file download to consumers who didn't want to download the operating system and inadvertently forced some users to upgrade earlier this year after it downloaded the files and began the installation process. The outcry from users who either didn't want to upgrade or couldn't, due to software incompatibilities or other W10 problems, has been significant — but Microsoft is not changing course. According to a new blog post, the company will be shifting Windows 10 into the "Recommended" update category, which means that users who have automatic updates enabled will receive the software automatically.

Microsoft Announcement:

"*Early next year, we expect to be re-categorizing Windows 10 as a "Recommended Update". Depending upon your Windows Update settings, this may cause the upgrade process to automatically initiate on your device. Before the upgrade changes the OS of your device, you will be clearly prompted to choose whether or not to continue. And of course, if you choose to upgrade (our recommendation!), then you will have 31 days to roll back to your previous Windows version if you don't love it.*

*If you are on a metered connection on Windows 7 or Windows 8.1, then you have the option of turning off automatic updates. We strongly discourage this in today's connected world because of the constant risk of internet threats.*"

The Windows 10 update does not apply to domain environments but certainly affects non-domain managed businesses and personal environments. Users on metered connections who may not be able to afford to download Windows 10 have to choose between manually controlling updates and paying overage charges. Meanwhile, customers who aren't interested in the operating system will have to jump through hoops to disable the upgrade after Microsoft goes to the trouble of downloading a 6GB file for them. While the company claims users will have the option to opt-out, people who don't know this is coming will simply get socked with it. So, be careful if your tendency is to click first and call for help once something goes wrong.

**Topic 2: TalkTalk Breached by Hackers**

British telecoms company TalkTalk has published information regarding the details accessed by hackers in the recent data breach.

Shortly after launching an investigation into the incident, TalkTalk attempted to downplay the incident saying that the attackers only breached its website and not its core systems, and that the amount of data exposed is significantly smaller than initially believed.

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

The company has now revealed that the hackers gained access to less than 21,000 bank account numbers and sort codes, less than 28,000 credit and debit cards, and less than 15,000 dates of birth. As it stated earlier in the investigation, the payment card numbers compromised in the breach are incomplete (i.e. six middle digits are blanked out), which means fraudsters cannot use the information directly to steal money from bank accounts.

TalkTalk also reported that the attackers accessed the names, email addresses and phone numbers of less than 1.2 million customers. The data, allegedly obtained by hackers after exploiting a SQL injection vulnerability, has been reportedly sold on cybercrime forums.

All affected individuals will be contacted and informed about the type of information that has been compromised.

"As we have previously confirmed, the credit and debit card details cannot be used for financial transactions. In addition, we have shared the affected bank details with the major UK banks so they can take their usual actions to protect customers' accounts in the highly unlikely event that a criminal attempts to defraud them," TalkTalk said on Friday. "We also encourage you to take up the free 12 months of credit monitoring alerts with Noddle, one of the leading credit reference agencies."

While the compromised data cannot be used directly to steal money from accounts, it can be highly useful for social engineering attacks, and now that TalkTalk told customers to expect to be contacted, such schemes could become even more successful. TalkTalk users have been warned that scammers and cybercriminals might leverage the recent incident to trick them into handing over bank details and passwords (TalkTalk says it will only ask for two digits), and installing malicious software.

The moral here is that often large security breaches occur for the purposes of selling user information to nefarious entities. Should you fall victim to such an attack make sure you are very careful in divulging any information to any entity regardless of what information they might have.

***Questions?***