Monthly InfoSec Newsletter

November 2020

Risky QR codes

Quick response codes or QR codes (above image) are scanned by phones to bring you to a website or display text. A growing scam is the replacement of QR codes at restaurants, so you think you are bringing up a menu, but the hacker has hooked you. After scanning a malicious QR code the hacker can add themselves as a contact, make you call the hacker, so they have your number, text or email your contacts, make a payment to the hacker, or reveal your location to them.

Some steps that you can take to minimize your risk are physically inspect the QR code paper and ensure that another code hasn't been pasted on top of the legitimate code. Be sure to only scan links from trusted sources and check the URL of the link once it has been scanned.

Windows 7 to 10

As many of you may know Windows 7 is no longer supported by Microsoft. Windows 10 is the operating system that Microsoft is currently supporting and providing monthly security updates. At CSU Pueblo, the IT team is working hard to upgrade all Windows 7 computers to Windows10. Users will be notified, a week ahead of time, when their machines will be upgraded. This process takes place automatically overnight to reduce the impact on user downtime. These security updates are a critical part of helping to prevent malware and vulnerabilities in Windows and associated software.

Security tips

For our security tip this month we are sharing a tool that will help you keep your machine safe, by allowing you to update your third party software applications with the click of a few buttons. The tool is PatchMyPC https://patchmypc.com/home-updater and is free to users for home use. It comes highly recommended by many working professionals who are now working from home due to COVID-19. PatchMyPC can all be downloaded and installed automatically. You can read customer testimonies here https://patchmypc.com/customer-testimonials

Thank you for reading our monthly InfoSec newsletter! We would love to hear some feedback from you, whether it's things you would like us to include or some criticisms you have. Please feel free to email us at infosec@csupueblo.edu and we hope you will continue to read our monthly newsletters!

Quick tips to help prevent QR phishing

- *Physically check QR code*
- *Only scan codes from trusted sources*
- *Check URL from the scanned code*

"84% of people have scanned a QR code before, with 32% most recently having scanned a QR code in the past week and 26% most recently having scanned a QR code in the past month."