Lewis University 90 years 1932-2022

OFFICE OF TECHNOLOGY

The Tech Connection

"Technology related news, information, and updates"

50th Publication

OCTOBER 2022

this month's issue

What is a Metaverse?

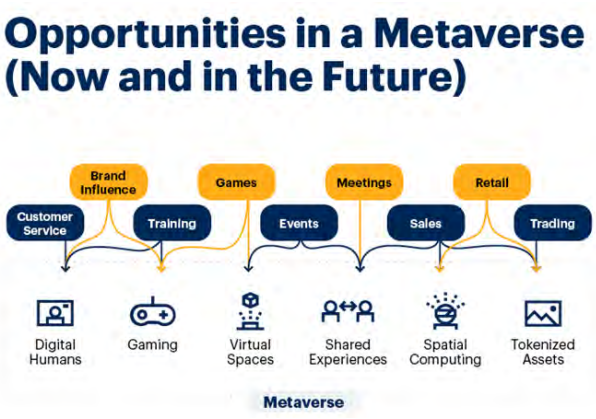
Many of you have probably been hearing the word "Metaverse" recently and may be wondering what it actually means. An article published by Gartner.com earlier this month explains that technically, a metaverse is a collective virtual shared space, created by the convergence of virtually enhanced physical and digital reality. For simplicity's sake, think of a metaverse as the next iteration of the internet, which started as individual bulletin boards and independent online destinations. Eventually these destinations became sites on a virtual shared space - similar to how a metaverse will develop.

A metaverse is not device-independent, nor owned by a single vendor. It is an independent virtual economy, enabled by digital currencies and non-fungible tokens (NFTs).

As a combinatorial innovation, metaverses require multiple technologies and trends to function. Contributing trends include virtual reality (VR), augmented reality (AR), flexible work styles, head-mounted displays (HMDs), an AR cloud, the Internet of Things (IoT), 5G, artificial intelligence (AI) and spatial computing.

4 key innovations make metaverse a strategic technology trend:

Innovation No. 1: Web3, which is a new stack of technologies for the development of decentralized web applications that enable users



to control their own identity and data. Web3 and metaverse complement each in a community or ecosystem where value in some form is exchanged between people or organizations — or a combination.

Innovation No. 2: Spatial computing, which can be defined as a three-tiered technology stack through which users experience the intersection of the physical and digital worlds.

Innovation No. 3: Digital twin of a person (DToP) not only mirrors a unique individual, but is also a near-real-time synchronized multipresence, with the ability to be present in multiple places at the same time in both digital and physical spaces.

Innovation No. 4: Digital twin of a customer (DToC), a subset of DToP, is a dynamic virtual representation of a customer that simulates and learns to emulate and anticipate behavior. Customers can be individuals, personas, groups of people or machines.

In short:

"The" metaverse doesn't yet exist. A metaverse today comprises multiple emerging technologies that promise the next level of interaction in the virtual and physical worlds.

Opportunities are emerging fast, but organizations should be careful when investing in a specific metaverse, as it is too early to determine which are viable for the long term.

(Click here to read the full article)

Physical Security is Important

UPDATE - This article was first published in our newsletter back in February. But…regretfully…I feel we need to publish it again. Over the last few months, I've noticed some bad habits I could not ignore. Just in walking about the LRC, I've found; a) rear office doors open with papers on a common table (nobody was in sight or saw me when I entered), b) physical keys left in a closed door and c) papers left in a busy hallway that had student information on them for over 15 minutes (I watched them after I found them and yes, they could have been left by anybody, but we need to be aware enough to handle them responsibly when we see them). Physical security is important.

The physical security for your area is important for information security. Protecting important data, confidential information, networks, software, equipment, facilities, university assets, and personnel is what physical security is about. The physical threats to information could be a malicious actor, fire or just a curious person. Any of these could cause harm and interrupt business. As you go through your day, think about the environment around you and these suggestions.

- Destroy physical copies of information as soon as they have served their purpose. Do not just discard them in an open trash bin.
- Lock drawers, computers, doors, and cabinets when not in use. Do not leave windows open if you will not be in the area for any length of time.
- Don't leave objects (documents, phones, purses, etc.) loose on desks or counters. Don't leave documents on the copier or fax machine for later.
- If you work on a lot with private or secure information, consider security film for your monitor. When you look around your area, are monitors facing 'common areas' or open windows? If so, consider moving the monitors/computers.
- Only authorized people should have access to offices unattended. Unauthorized people should not be allowed freely into offices, access to copiers, or use of desk space.
- If you see something, say something. Security issues need to be addressed promptly.
- Make sure you understand any fire protections or procedures for your area. For instance – where are the fire extinguishers, what is your exit path from the building, or who do I contact.
- Is the light in your office area sufficient? You do not what any areas that are dim as items can be easily overlooked.
- We cannot improve if we cannot identify a problem; always communicate with your manager if you have questions or ideas.

If you have questions or ideas, please talk to your manager or contact the Service Desk.

FALL SEMESTER TECHNOLOGY SUPPORT

PHONE SUPPORT: On Campus: Extension 5950 | Off Campus: 815-836-5950

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
1:30am - 10pm	7:30am - 10pm	7:30am - 10pm	7:30am - 10pm	7:30am - 10pm	7:30am - 5pm	9am - 5pm

WALK-UP SUPPORT: Lower Level LRC

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
	7:30am - 5pm	7:30am - 5pm	7:30am - 5pm	7:30am - 5pm	7:30am - 5pm	

EMAIL: servicedesk@lewisu.edu | ONLINE: https://servicedesk.lewisu.edu

Tips for Staying Safe with URLs

You use URLs every day. They are the nice names for the common resources you use on the Internet (i.e., www.facebook.com or www.outlook.com). While you use them to make your life simple, hackers can use them to gain access to your machine or collect information. Do you pay close attention to URLs you receive in emails or texts? Do you know what every site does or where it goes? Most likely you don't. It is always important to think before you click. To help with that, follow these few tips and maybe you won't fall for a scam.

- ⇒ Hover your mouse over links before you click. When you hover your mouse over a link, you will be able to see the URL you will be taken to if you click.
- ⇒ If you receive an email with a link, navigate to the organization's website in your browser instead of clicking the link. By visiting the organization's website directly, you can ensure that the deal or promotion is legitimate.
- ⇒ Before you click a shortened URL, make sure it is legitimate. You can use an online URL checker to view the full URL (like https://iplogger.org/url-checker/).
- ⇒ If you want to see if a URL is safe, you can check them online before clicking (we use https://www.virustotal.com).

Other Free Online Tools that Check URLs

- AbuseIPDB: Provides reputation data about the IP address or hostname
- Auth0 Signals: Checks IP address reputation; supports API
- BrightCloud URL/IP Lookup: Presents historical reputation data about the website
- CheckPhish: Checks whether the URL is a fraudulent site
- CyberGordon: Look up the website (and other observables) across several services
- Desenmascara.me: Flags websites suspected of selling counterfeit products
- Email Blocklist Checker: Checks the domain name or IP address against email blocklists (email address required, opts into marketing).
- FileScan.io: Examines the URL in real time
- FortiGuard lookup: Displays the URL's history and category
- Google Safe Browsing: Look up the website's current status
- hashdd: Provides historical data about IPs, URLs, etc.
- IBM X-Force Exchange: Provides historical data about IPs, URLs, etc.
- IPQualityScore: Presents a risk ranking for the IP address
- Joe Sandbox URL Analyzer: Examines the URL in real time
- Ironscales Fake Login URL Scanner: Examines the URL for signs of phishing
- Is It Hacked: Performs several checks in real time and consults some blacklists
- IsItPhishing: Assesses the specified URL in real-time

(Click here for the full list)

QR Codes - Do you know Where They Go?

Maybe you've seen this around the campus. I've found a few small piles left in bathrooms and on tables. If you did, did you scan the code? You know where it goes? You know what the site could do? Stop. Think. Connect.

Before you scan a QR Code you should ask yourself:

Where does the information from QR Codes go? In the QR code, the arrangement of the squares—or data modules, as they're called - is actually a URL. It's just been translated from the alphanumeric string of the URL into a collection of squares. That's how you go from link to QR code. A QR code scanner will then translate it back to the original URL.

Can a QR code hack your phone? "Cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use – Do not scan a randomly found QR code."

Why shouldn't you scan QR codes? The QR code's URL can take you to a phishing website that tries to trick you into entering your username or password for another website. The URL could take you to a legitimate website and trick that website into doing something harmful, such as giving an attacker access to your account.

What happens when you scan a QR code with your smartphone? Scanning these modern-day barcodes with your smartphone lets you quickly open a web page, download an app, send a text message, and much more. Many restaurants and bars are even replacing their menus with QR codes, while some stores allow you to pay with a QR code now, so you don't have to touch anything.

(Click here for further information on QR Codes)