Star tribune
wed 12/9/2020

Photos by MARK MA

s on Etsy while on leave from her job as a flight attendant with Ame

lace on Wall Street

nother pandemic success story.

sts around
e and vin-
il, she has
sks, raking
ometimes,
norning to

blessing,"
something
of thinking

nasks have
year. The
business
kes of Pan-
d Etsy into
d: a Wall

Along with a cluster of "stay at home" stocks such as Zoom Video, Peloton and Shopify — so called because their businesses took off during the pandemic as people's shopping and work habits changed — Etsy has seen its share price soar.

More than 90% of Wall Street analysts rate the stock a "buy." Individual investors, mutual fund managers and hedge fund traders alike have been scooping up its shares, which have risen more than 250% this year.

That makes Etsy by far the best-performing stock in the S&P 500 stock index, to which it was added

See **ETSY** on D4 ►

Kat Panchal has raked in more than $4,500 selling her face masks.

tech to help arm movement

ilitech photo

e.

The firm's wearable device is designed for people with neuromuscular disorders.

By NEAL ST. ANTHONY
neal.st.anthony@startribune.com

Abilitech Medical Inc., the Minneapolis medical device startup that won the Minnesota Cup last year, on Tuesday said it launched Abilitech Assist, a cornerstone product in its plans for wearable tech that helps people with limited movement in their arms.

"This has been my dream for over four years," Angie Zavoral Conley, the company's founder and chief executive, said in an interview.

"Our device allows the arm and shoulder to move effortlessly, much like in a swimming pool," she said. "We work with [patients], clinicians and caregivers. This includes input from an engineer on our team who lives with a spinal cord injury."

The Assist supports the shoulder and elbow, and software customizes a "spring tension" to lift light objects such as a fork, phone or water bottle.

The Food and Drug Administration classified the Assist as a wearable product, which allowed Abilitech to commercialize it at the same time it continues clinical trials at the University of Minnesota and Gillette Children's Specialty Healthcare. Other collaborators include HealthPartners and Allina Health's Courage Kenny Rehabilitation Institute.

See **ABILITECH** on D4 ►

Millions of devices vulnerable to hacking

In worst case, critical services such as water and power could be crippled, researchers say.

By FRANK BAJAK
Associated Press

BOSTON – Researchers at a cybersecurity firm said they have identified vulnerabilities in software widely used by millions of connected devices — flaws that could be exploited by hackers to penetrate business and home computer networks and disrupt them.

There is no evidence of any intrusions that made use of these vulnerabilities. But their existence in data-communications software central to internet-connected devices prompted the U.S. Cybersecurity and Infrastructure Security Agency to flag the issue in an advisory.

Potentially affected devices from an estimated 150 manufacturers range from networked thermometers to "smart" plugs and printers to office routers and healthcare appliances to components of industrial control systems, the cybersecurity firm Forescout Technologies said in a report released Tuesday. Most affected are consumer devices including remote-controlled temperature sensors and cameras, it said.

In the worst case, control systems that drive "critical services to society" such as water, power and automated building management

See **CYBERSECURITY** on D4 ►

12,582.77 ▲ 62.83 | **10-YR T-NOTE** 0.90% ▼ 0.01 | **GOLD** $1,870.80 ▲ 9.00 | **OIL** $45.60 ▼ 0.16 | **EURO** in dollars 1.2103 ▼ -.0017

shut down at different ti
throughout the pandemic

At the same time,
report from the U shows
women in Minnesota are
highly represented in m
of the high-risk essential

Star Tribune
wed 12/9/2020
-continued-

ed that the state could see
lar demographic dispari-
this winter from the new
osses.

a Kumar • 612-673-4113
er: @kavitakumar

Millions of devices could be vulnerable to hacking

◂ **CYBERSECURITY** from D1

could be crippled, said Awais Rashid, a computer scientist at Bristol University in Britain who reviewed the Forescout findings.

In its advisory, CISA recommended defensive measures to minimize the risk of hacking. In particular, it said industrial control systems should not be accessible from the internet and should be isolated from corporate networks.

The discovery highlights the dangers that cybersecurity experts often find in internet-linked appliances designed without much attention to security. Sloppy programming by developers is the main issue in this case, Rashid said.

Addressing the problems, estimated to afflict millions of devices, is particularly complicated because they reside in so-called open-source software, code freely distributed for use and further modification. In this case, the issue involves fundamental internet software that manages communications via a technology called TCP/IP.

Fixing the vulnerabilities in impacted devices is particularly complicated because open-source software isn't owned by anyone, said Elisa Costante, Forescout's vice president of research. Such code is often maintained by volunteers. Some of the vulnerable TCP/IP code is two decades old; some of it is no longer supported, Costante added.

It is up to the device manufacturers themselves to patch the flaws and some may not bother given the time and expense required, she said. Some of the compromised code is embedded in a component from a supplier — and if no one documented that, no one may even know it's there.

"The biggest challenge comes in finding out what you've got," Rashid said.

If unfixed, the vulnerabilities could leave corporate networks open to crippling denial-of-service attacks, ransomware delivery or malware that hijacks devices and enlists them in zombie botnets, the researchers said. With so many people working from home during the pandemic, home networks could be compromised and used as channels into corporate networks through remote-access connections.

Forescout notified as many vendors as it could about the vulnerabilities, which it dubbed AMNESIA:33. But it was impossible to identify all affected devices, Costante said. The company also alerted U.S., German and Japanese computer security authorities, she said.