DTS DanTech Services
Computers under control!™

Technology Times May 2020 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

Life after Covid-19—Protecting yourself wherever you work

By Dan Foote, DanTech Services, Inc

People respond to all kinds of manipulations. Marshall McLuhan recognized this in the early 1960's when he introduced his Understanding Media: The Extensions of Man where the phrase "the medium is the massage" originated via a mistake by his graphic designer for what should have been "the medium is the message". Social engineering is exactly that massage of the human psyche where victims are enticed, coerced, or manipulated into a response that can have disastrous implications to their safety, data, finances, and health.

Readers of our newsletter will know that we've covered social engineering in the past. We will likely cover it in the future, too. The subject is that important and, just like any difficult class you've taken, repetition improves retention.

Whether it's baiting, phishing, spear phishing, pretexting, quid pro quo, vishing, smishing, or simply being friendly to someone, social engineers are generally after one of the following: data (information that can be used for gain), access (to an area or service that can be exploited), or profile building (which is a form of information gathering).

Recently, we received a call from a person looking for help. He was offered something for nothing, as it turned out. In a classic "quid pro quo" scheme, the victim was offered a sum of money if he provided the SE (social engineer) access to his Facebook account. The nothing was in the form of no money and no more access to his Facebook account. Some might say, "big deal." I'll say, "yes, it is a big deal." The SE now has the ability to reach out to FB friends, family, and contacts under the pretext of trust. Please be a good steward of the trust that others place in you through your social media channels—and don't trust anybody that wants access to your accounts. In short, it's OK to be cynical and skeptical to all requests that come by phone, email, website, text, or personal requests.

- Continued on page 3

The top ten remote worker frustrations

1. Slow internet speeds. The biggest problem facing mobile workers? Simple. Networks just aren't fast enough. Compared to well-resourced corporate networks, it seems that 4G and public or home WiFi hotspots just don't offer enough speed to reliably get work done.

2. Undiagnosed network problems. A huge frustration for many employees is when they just can't seem to get thier internet connection to work. Responders cited a handful of common examples, such as devices show a strong connection but online services failing to connect. Despite apparently being connected, all too often websites will not load, and real-time apps won't work at all. Annoying.

3. Network disconnects. It's no surprise that mobile working typically involves being physically mobile too. When switching between different types of networks, often the connection is dropped altogether. The same happens in rural or congested areas. Dropping out of a network like this is the third-most frustrating issue for mobile workers.

4. Terrible mobile functionality. A call to arms to mobile app developers: replicate your desktop feature sets. Ranking high among remote workers is the reality that the mobile counterpart to desktop systems will frequently provide weaker functionality – an understandable frustration for those trying to work on a smartphone in particular.

5. Authentication and login issues. Specific policies will vary at each organization, but a common thread for workers was the pain of having to authenticate and re-authenticate to corporate systems. Overbearing password enforcement policies, multi-factor authentication and having to re-login whenever a connection is dropped all contribute to this major frustration.

6. Devices crashing and restarting. Even the highest spec smartphones and laptops will start to struggle with performance after a few years. A large number of workers cite failing hardware when it comes to factors that negatively impact employee experience.

7. Insufficient battery life. Another sign of failing hardware is recurring issues with battery. That two-day charge can quickly become that two-hour charge if devices are used heavily and start to show signs of age.

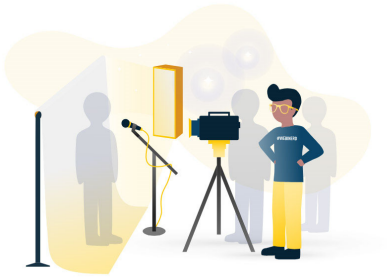
8. Online session timeout. The rise of real-time applications and websites that require and always-on connection has been significant – from VDI to cloud platforms designed to foster better collaboration. The trouble for remote workers is lost productivity whenever a session is restarted due to an unwanted changing network condition.

9. Using public WiFi. The proliferation of public WiFi has been great for offloading devices from LTE networks and improving the availability of an internet connection. One of the frustrating consequences of this has been that bypassing the login or T&Cs of these networks is seen by mobile workers as significantly hampering the user experience.

10. Unable to access work tools. Whether it's a cloud platform like Office365 or a traditional setup requiring the use of a VPN, a popular concern among mobile workers is getting access to the data that matters.

Virtual "Video" Meetings as Theatre

By Mary M Rydesky, VP, DanTech Services, Inc



Leading or participating in a meeting is commonplace now – we use Zoom, Skype, Teams, WebEx, Collaborate, and other programs that allow us to see as well as to hear one another. Remember the phrase, "lights, camera, action"? Here are ideas for improving the quality of your presence.

Lighting

- Turnoff/cover/remove light sources located behind you – including light coming through a window. Also, avoid having an overhead light above or behind you.
- Place a lamp behind your web cam for soft, indirect lighting of your face.

Staging

- What can be seen behind you? Your viewers are looking – does the 'look' relate to the image of your business.
- Values - do you want to convey attention to detail or dependability – or the chaotic state of your bedroom or kitchen? Consider how organized the background appears. If there is art work or white boards in the background, make certain you want viewers to see what you have there. Same for book titles and items sitting on shelves.

Costume

- Are you wearing your best colors? Is the style effective for the purpose of your meeting?
- Color near your face will enhance your image of being healthy and energetic. Consider ties, scarves, turtlenecks in strong solid colors if these accessories suit your style.

Camera

- Angle the web cam so that your viewers see your head and shoulders rather than the ceiling.
- Consider the 'gut shot' if you stand up/sit down in front of the camera, what does the viewer see? Cover or close your camera before moving.
- Use a camera cover when not in a virtual meeting – and close it before you give a 'gut shot'.

Sound

- Your goal is to have your sound come across as what you hear on a good newscast. Speak clearly – slowly and loudly enough to carry.
- Curb ambient noises – fans, dishwashers, family members, doorbells, car door sounds, other distractions. Perhaps posting a sign would alert others to keep quiet.

To read a full document please click here.

Call **907-885-0500** if you have any questions about **Work From Home** setup, network and connectivity problems, need Teams to work and more!

"Life after Covid-19—Protecting yourself at work or at WFH"
- Continued from page 1

Alaskans understand the idea behind chumming. That's our phrase for baiting, where we might throw or place a tasty morsel for fish or wildlife as an attraction. The same principal applies to finding "lost items" that can be used to exploit a computer. Finding a USB flash drive in a building, parking lot, or on the street can be a temptation of our curious nature to see what's on it. While there are ways to explore a USB drive without compromising your computer security, leave that to the experts. Simply plugging that found item into your computer can unleash ransomware, trojan, keylogger, or some other threat. Doing this on a business network can shut down the business. The costs can be in the millions of dollars—not to mention jobs.

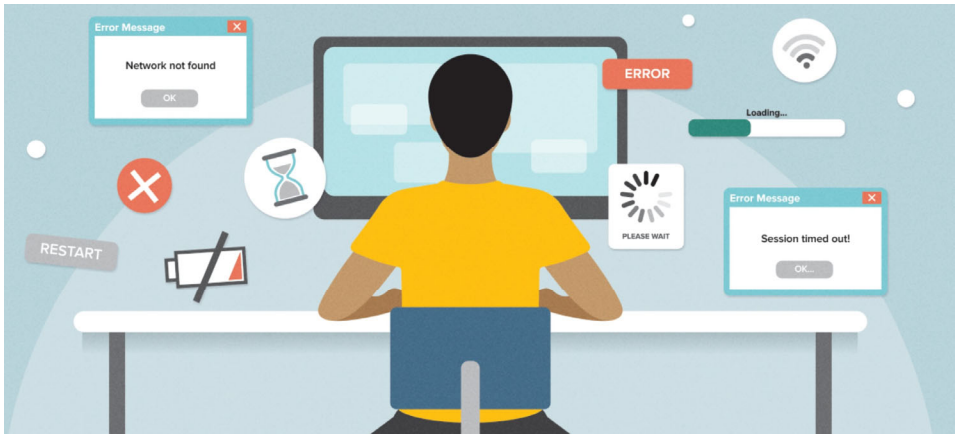
Protection basics can include the awareness of how to inspect a weblink, exercising extreme caution when something sounds too good to be true, ignoring that sense of urgency that "this needs to be done now!", or simply wanting to hold a door for someone—especially if it leads to a restricted area.

Artificial intelligence has gained ground in increasing exploit effectiveness. Change how you answer your phone when you don't recognized the calling number. When I'm asked, "Is this Dan?", my response is, "How can I help you?" Why do I do this? Because answering "Yes" might get my voice recorded to where the SE can reuse that word to gain access to accounts or services where voice-print matching is used.

I'll repeat: you are far better off being cynical and skeptical of offers or enticements. Of curiosity. In a world where we find that the "medium is the massage" at every turn, protect yourself, your family, and your friends & co-workers through caution. In this day of COVID-19 and all of the scams that have been unleashed, it's your data—your information—that needs to be protected.

Our offer to you is this: before you respond to something that seems to be "legit", give us a call. We'd be happy to see how legit it really might be.

New Residential Support Service Announced!



For less than $2.00 a day, keep your home network and computers protected & worry free!

Get support for up to 3 computers and your home network. We will provide management and monitoring, patch updates, anti-virus, and remote support. No long term contract. *Additional services available. **Restrictions apply.

CALL 907-885-0500 TO GET YOUR 2 MONTH DISCOUNT!

Shiny New Gadget Of The Month:

Asus MiniPC PN62

While laptops are excellent for moving between meeting rooms, they are otherwise uncomfortable due to the poor positions of their keyboards and excess heat. The Asus MiniPC PN62 is a small but powerful productivity machine is a good option for **Work From Home** that the boss might even pay for. Just plug it into a wall socket and add an external monitor.

The presence of a 10th Gen Intel processor and solid-state drive (SSD) means the MiniPC PN62 performs very well for productivity tasks. The MiniPC PN62 offers a full plethora of ports that includes multiple USB 3.1 ports, gigabit LAN, an optional Thunderbolt 3 port, as well as built-in Wi-fi 6 and Bluetooth 5 with no visible antennas. RAM can go up to 64GB and there is even space to add a 2.5-inch storage drive for additional storage capacity.

While the MiniPC PN62 is typically whisper quiet, the high-pitched whine of the CPU fan means it can get audible when under heavy load. Toggling "Max Power Saving" mode from the Asus Business Manager app keeps it so quiet you forget it's there.

Price: from US$618

4 Steps to Move your Business from Defense to Offense During Times of Disruption

By Andy Bailey, Petracoach

"Everyone has a plan until they get punched in the mouth." – Mike Tyson.

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID, the annual or quarterly one you had is now likely irrelevant.

You have two options:

1. Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let's face it, that's not happening).

2. Create and act upon a new game plan. One that's built to overcome disruption and transform your business into something better and stronger.

Option 2 is the correct answer!

It's D.S.R.O pivot planning process.

It stands for **Defense, Stabilize, Reset** and **Offense**. It's a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn – better and stronger than before.

Here's a shallow dive into what it looks like:

Defense. A powerful offensive strategy hinges on a strong defense. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

Stabilize. The secret to stabilization is relentless communication with everyone. That includes internally with your teams AND externally with your customers. Streamline communication and eliminate bottlenecks through a visual dashboard.

Reset. By completing the first two steps, you'll get the freedom you need to re-prioritize and focus your efforts on the most viable opportunities for growth.

Offense. Don't leave your cards in the hands of fate. Shifting to offense mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

I'll leave you with this statement from top leadership thinker, John C. Maxwell. It's a quote that always rings true but is crystal clear in today's landscape.

"Change is inevitable. Growth is optional. "

Dark Web Scan Assessment

As CEO of an Alaskan WFH Business, How Do You Safeguard Your Company's Data And Your Customer's Private Information?

Get FREE Dark Web Scan Assessment—call 907-885-0500