10 Things You Need to Know About Data Security & Working Remotely

G. Kevin Roper, MBA
Chief Operating Officer
Cynergy Technology

kevinr@cynergytech.com
https://www.linkedin.com/in/gkevinroper/
903.720.2032 mobile

DO - USE AVAILABLE TOOLS

Use remote connectivity tools to stay in touch with clients and keep business processes flowing.

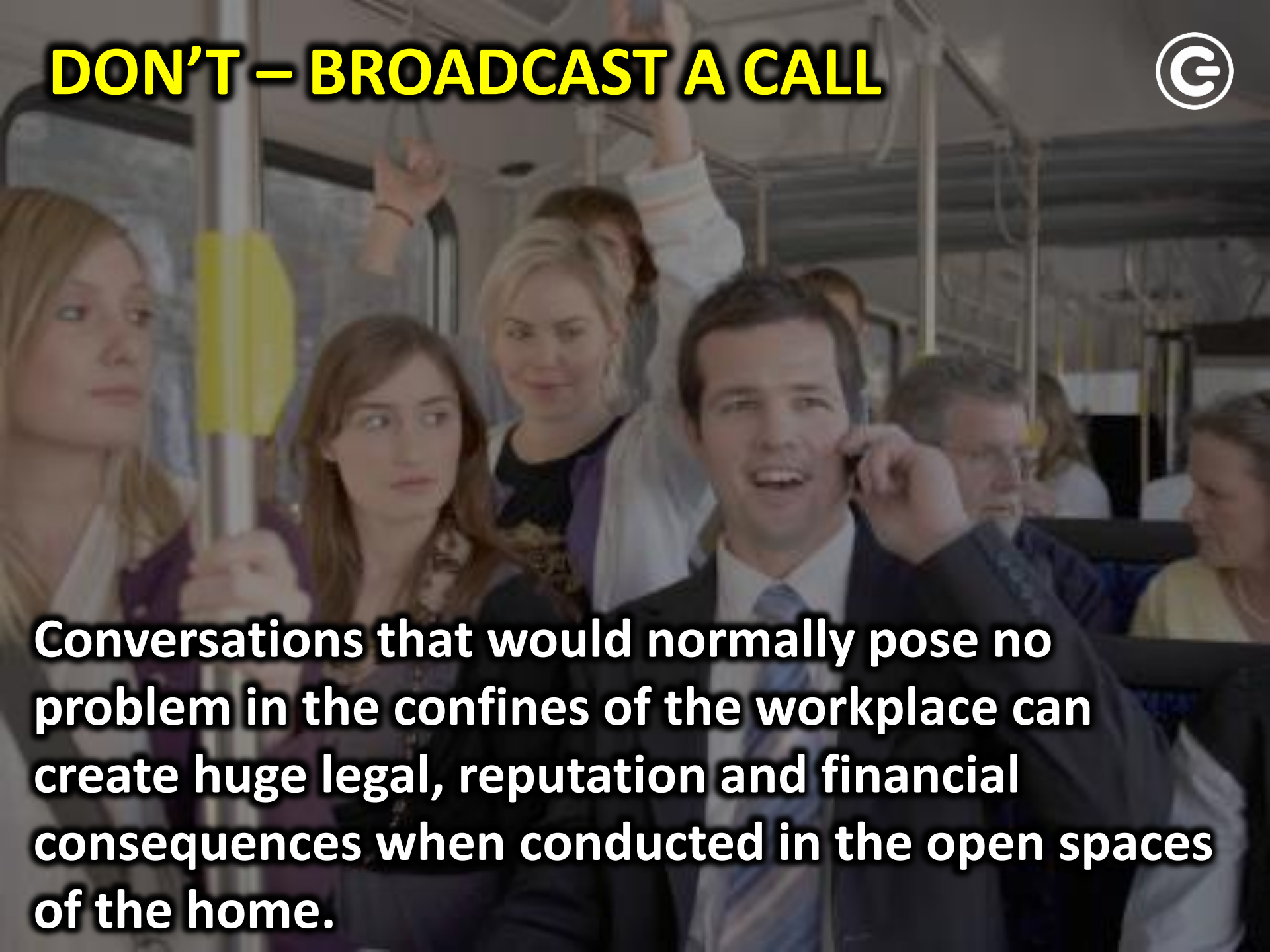
DON’T - USE SHARED COMPUTERS

Don’t access critical business, financial or medical systems from a shared computer the family uses that may already be compromised.

DON'T – PRINT SENSITIVE DATA

Don't print sensitive documents unless you can immediately secure them from unauthorized viewers.

DON'T – BROADCAST A CALL



Conversations that would normally pose no problem in the confines of the workplace can create huge legal, reputation and financial consequences when conducted in the open spaces of the home.

DON'T – FALL FOR EMAIL SCAMS

Pay special attention to any email containing a link. Ask yourself this question: *was I expecting this email from this person today?*

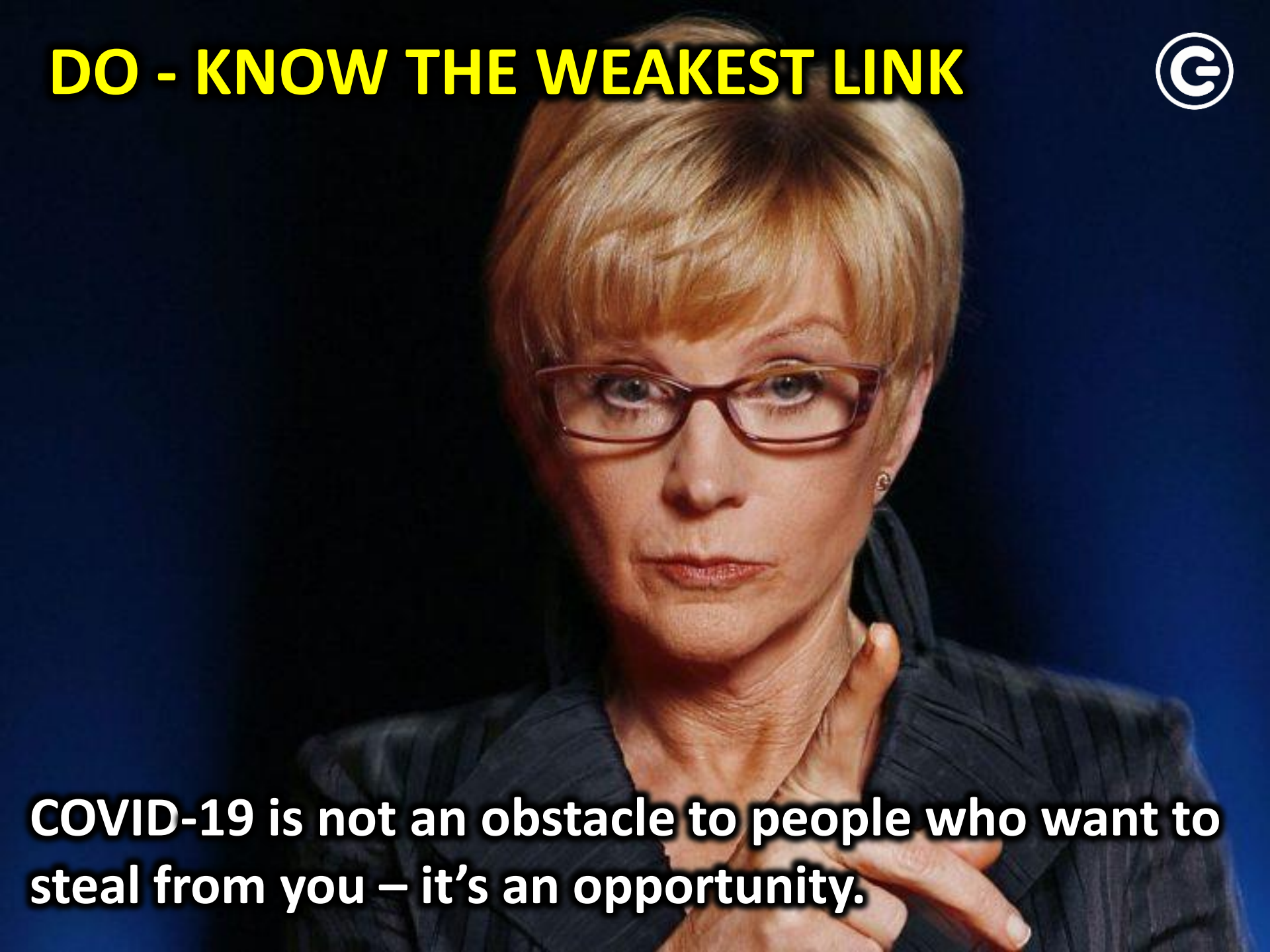
DO – LOGOFF YOUR COMPUTER

If you have to walk away from your workspace - even for a minute (which may turn in to 10 to 20 minutes) – log out.

DO – USE SECURITY MEASURES

VPNS, WPA2 and Bears…Oh My! We are not in Kansas any more, Dorothy…

DO - KNOW THE WEAKEST LINK

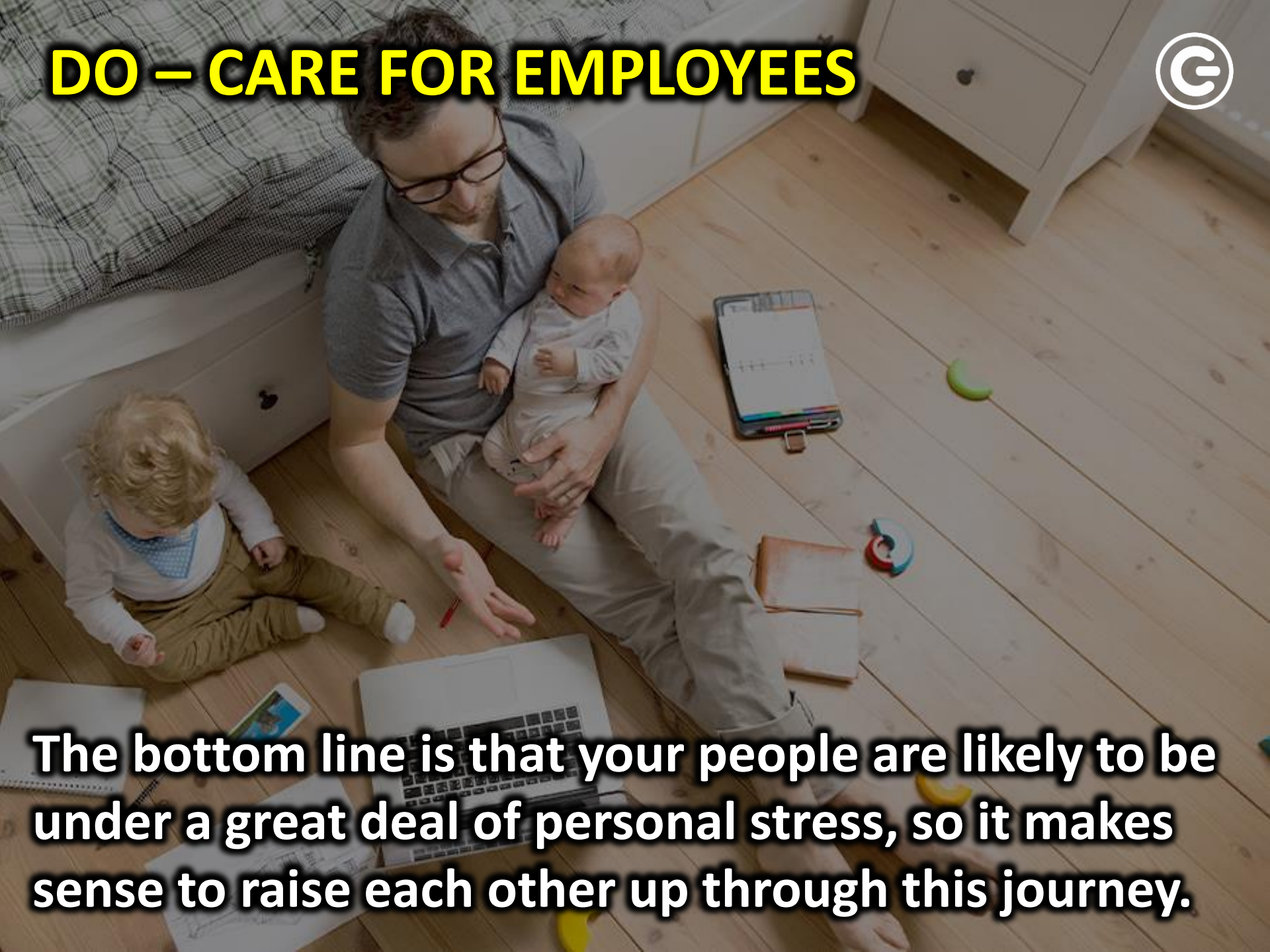


COVID-19 is not an obstacle to people who want to steal from you – it's an opportunity.

DO – TALK ABOUT SECURITY

Talk to your IT department or managed service provider about security measures.

DO – CARE FOR EMPLOYEES



The bottom line is that your people are likely to be under a great deal of personal stress, so it makes sense to raise each other up through this journey.

https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom

https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine

https://www.usatoday.com/story/tech/columnist/2020/04/04/coronavirus-scams-going-viral-attacking-computers-and-smartphones/2939240001/

https://www.tripwire.com/state-of-security/security-awareness/covid-19-scam-roundup-april-6-2020/

https://staysafeonline.org/covid-19-security-resource-library/

WE CAN HELP – GIVE US A CALL

THE CHANNEL CO.
CRN
MSP 500
2020

The 2020 Managed Service Provider 500

The Top Managed Service Providers and Consultants in North America

CRN's Managed Service Provider 500 list recognizes the top technology providers and consultants whose forward-thinking approach to providing managed services is changing the landscape of the IT channel.

Cynergy Technology has been named to the **MSP Pioneer 250** list. The MSP Pioneer 250 have largely built their business model around providing cutting-edge managed services to the SMB market.

For more information on how your business or organization can benefit from Cynergy Technology's wide array of services and solutions, contact us at:

903.581.7000 (Tyler office)
903.757.5900 (Longview office)
www.cynergytech.com

Use remote connectivity tools to your advantage to stay in touch with clients and keep business processes flowing.

Like any tool, always employ best practices in the way you use it

if you don't know what those are – get help from a reputable IT provider.

For example, Zoom meetings are a hot topic today.

Reading the news, you may hear warnings about Zoom video conferencing.

Some large organizations are banning its use entirely.

Again, its like any tool – use it incorrectly or unsafely, get bad results.

Works great if you follow best practices.

If you use Zoom (or any video conferencing service), be sure to:

download the latest client

don't publish the meeting number or private password to public forums *(yes, some students did this)*

add security or waiting rooms to all meetings – Zoom has just made this the default for new meetings

Don’t access critical business, financial or medical systems from a shared computer
This is equally true for USB thumb drives you have around the house – be very careful with them
- family computers may already be compromised. USB drives may already be infected.
- That funny cat video the kids clicked on…the free app your spouse downloaded
- Hackers love viral videos and “free” downloads for carrying things you didn’t know were there

If a hacker has installed a keystroke logging package on your unsecure family computer or USB drive, they can get the login and password to your most sensitive business systems.

Use a business computer or have your IT department or vendor inspect your home computer before use.
Have that USB drive thoroughly inspected BEFORE you plug it in.

Business computers and IT departments and vendors know what to look for:
- antivirus that is fully patched
- operating systems with security enabled and updated
- connections to the internet that are secure
- files scanned and tested

Don’t print sensitive documents unless you can immediately secure them from unauthorized viewers.
If you must print, don’t throw away documents – shred them.

A note – as we go through the list, notice how many of these recommendations are “common sense” things
- you wouldn’t use a computer without updated anti-virus in your work place
- you wouldn’t print sensitive material and leave it in a break room at the office

This risk, like many others, is underestimated when working remotely because it is “our home”
- A safe place. A comfortable place.
- And because of that, a risk for critical data to get out in the open.

Failing to control sensitive printed information while working remotely at your dining table is no different than taking a secure file from the workplace and leaving it spread out at the local library.

Don’t have business phone calls to discuss patients, clients or workforce members where anyone else can hear confidential information.

Again, this is “common sense” at the office but may be overlooked in the living room

Conversations that would normally pose no problem in the confines of the workplace can create huge legal, reputation and financial consequences when conducted in the open spaces of the home.

Treat every business conversation as confidential and make sure the space you are using is private.

Google has recently reported a 350% jump in malware attacks. Phishing scams are up 667% in one month.

This morning, the Dept of Homeland Security, the Cybercrime and Infrastructure Security Agency and the UK's National Cyber Security Center released a joint global warning. A brief quote:

Groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

As frightening as that may sound, protecting yourself against it is relatively simple:

Don't fall for email scams asking for money transfers, sensitive information, gift card purchases, or payroll deposit redirections without TALKING to the person making the request to verify it.

Before you open it, ask yourself this question: was I expecting this email from this person today?

Pay special attention to any email containing a link. Some of the worst data disasters imaginable start with a single click in the wrong place.

If the email does contain a click, hover over it (don't click it).
Many times, a small popup box will tell you what the link will do if you click it.
Is that a place you really want to go?

Biggest piece of advice – SLOW DOWN. Concentrate and think about what you are about to open.

We talked earlier about not getting too comfortable at home with shared computers, phone conversations, and print materials.

Here is another “common sense” practice that should already be practiced in your office space:

Do log off or lock your workstation if you have to walk away from your computer – even for a minute, which may turn in to 10 to 20 minutes.

Do not leave sensitive information on the screen or critical business systems open and logged in.

I’ve done a full hour cybersecurity training all over the east Texas region.
One of the consistent questions I get is – is it OK to leave my computer on or logged in my locked office?
The answer – in your locked office or on your kitchen table – is NO…

- It’s the access you didn’t anticipate that will compromise your business.
- The person on the nightly cleaning crew with a key.
- The coworker who is about to quit and would like to take key information with him/her.
- The child who just wanted to watch the Disney Channel and hit the wrong button…

Be sure your workstation is secure if you are not on it.

Do use a secure connection to provide end-to-end encryption of data in transit.

This can be a VPN to the office

Think of this like moving $10 million from one place to another.

Sure, you can put it in the backseat of your Ford and drive it to the bank. It might get there safely.

Or, you can put it in an armored truck driven by people with machine guns.

VPNs give you added security and privacy.

Most current firewalls will do a good VPN if they are setup and tested correctly.

Other recommendations if you don't have a VPN:

Use a security filtering company that will verify web connection links for safety.

Stay off public wi-fi and stop using your neighbor's unsecured wireless signal (you know who you are…)

Update security on your home network.

Ensure you are using WiFi encryption (WPA2 is recommended).

Change the login and password on your router if possible.

If you are not using a home firewall, it's time to start using one.

Know this – the most effective weapon in the hacker's arsenal is not technical – it's social.

Socially engineered hacking is using what hackers know about you and your habits to get you to give them information they should not have so they can make money from it.

Here are 3 things I know about you (at work but maybe more at home) that helps me steal your money:

1. You move too fast. Your world is spinning 150mph. There is rarely enough time in the day.
2. You are distracted. Two incoming calls, 20 unanswered emails, 2 kids and 3 pets climbing on you.
3. You consume information using technology – one click at a time.

This is one place we can offer you totally free advice:

1. Slow down. Autopilot is a bad thing right now. Turn off the cruise control and ease up on the pedal.
2. One thing at a time. Let the call go to voicemail while you are processing your emails. It will wait.
3. Don't click until you think through it. Hover first.

It is a multi-trillion $ business and COVID-19 is not an obstacle to people who want to steal from you – it's an opportunity.

Talk to your IT department or managed service vendor about security measures.

Ask about subjects such as VPNs, multi-factor authentication, email encryption, sandboxing and backup/dr.

If they cant explain it in normal human language, find someone else to talk to

Some of your IT people or managed service vendors have been trying to talk to you about this for years

They will probably be happy you are interested in discussing it.

And remember – it's not only your company's security that should be assessed, but also any vendor that has access to your sensitive company systems. Ask them the same questions.

The reason many people are working from home is because there is a health pandemic.

The grim truth is that your employees may get sick, or worse, during this crisis.

With this in mind, community chat, including group video chat using tools such as FaceTime or Zoom, will become increasingly important to preserving mental health, particularly for anyone enduring quarantine.

I have heard of one group of people working remotely that are using a home exercise app and Group FaceTime to exercise together during the day, which they think helps boost team feeling even while working remotely.

While the technology is a good communication tool, it isn't a replacement for your concern for your team

Phones and emails are great for daily check in.

Keep up with your employees on facebook – people are sharing more than ever online. Comment. Like things.

if someone is sick, double your effort. A sniffle right now is a scary deal.

Keep employees updated. If you read something useful (business related or not), send it on. You are saying "I care"

The bottom line is that your people are likely to be under a great deal of personal stress, so it makes sense to raise each other up through this journey.