Five ways to thrive while working from home during the coronavirus pandemic

- **Fine-tune your work-at-home plan**
- **Morning is the prime time**
- **Dress for sucess**
- **Avoid distractions**
- **Telecommuting needs good gear**

With more than 100 million Americans told to stay at home – nearly one-third of the country's population – it has inexorably changed the way many of us work, play, learn and socialize.

At the very least, technology has proved to be an extraordinary tool to help us adjust to this new normal.

Especially for those mandated to work from home, there's no shortage of ways to remain productive while self-isolated or quarantined – but as many have likely discovered, it can be challenging at times. As someone who has worked from home for more than 25 years, I can attest to that.

Even if the situation is short term, the following are some thoughts on "best practices" while working from home.

Fine-tune your work-at-home plan
Working from home isn't a "one size fits all" scenario. Some people, for example, are "segregators" who need to be closed off from personal life (such as in a home office), while others are "integrators" who work better in, say, a kitchen, and with kids and pets around.

If you work better in the morning, work in the morning. If you have some flexibility and you get more done after the sun goes down, stick with that. Determine what works best for you, and embrace it. Be sure to take advantage of reliable technology to make your work more productive.

For most, morning is the prime time
Contrary to my first telecommuting tip, several studies have found those who get the bulk of their work done in the morning are more productive and successful than those who sleep in.

On a personal note, I try to get as much done before lunch as possible, which frees up time in the afternoon to prep well for the next day, go after new business (as a freelancer) or take a mental break, such as a jog around the block, before getting some more work done.

As someone who works from home, I often have trouble turning work "off," even at night, but be sure to set some time for yourself and family – especially when your partner or kids might be feeling anxious during these times of self-isolation.

Dress for your success
Unless you're video conferencing and need to be dressed in business casual or better, wear whatever makes you comfortable – even if it's sweatpants, T-shirt and baseball cap. Sit in a comfortable chair, in a room with good lighting. For those who spend a lot of time chatting on the phone for work, a hands-free headset is a more comfortable choice compared to holding a handset up to one's ear. This is especially true for those who like to multitask, such as typing on a computer while talking at the same time. Keep water at your desk to remain hydrated.

Avoid distractions
While it boils down to personal preference, having a home office is a good idea for a couple of reasons: You might work more efficiently without distractions, whether it's the tempting snacks in your kitchen, a loud television or hearing the kids argue over a toy. Closing a home office door means your colleagues or clients are less likely to hear the dog barking at a squirrel seen through a window. (Another tip: Get to know your phone's mute button, too.) And you might need a separate home office for any tax credits and write-offs you're looking for. Distractions are bad, but breaks are good. Take them, but then go back to work.

Telecommuting needs good gear
An essential item is a good computer, whether you choose a desktop with a large monitor or a portable laptop you can deploy throughout your home. Be sure it has a comfortable keyboard, a camera for video calling, and cybersecurity software to protect your (or the company's) information. A good backup solution is key, too, in case of a power outage (or surge), virus or hardware malfunction.
Source: USA Today

Coronavirus stimulus scams are here. How to identify these new online and text attacks

As with any public crisis, the spread of the coronavirus has created a new crop of hackers -- targeting people who are awaiting their stimulus check, who are working from home and who are just trying to stay healthy. Add in April Fools' Day and you need to be on guard against all kind of scams and misinformation found online, in your email inbox and even in your text messages.

A recent release from the FBI's Internet Crime Complain Center offers some solid advice on what to watch out for.

"Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them," the FBI said. "Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits."

New research from Next Caller found that about 32% of 1,000 surveyed Americans believe they've already been targeted by fraud or scams related to COVID-19. Next Caller also found that fraud concern is increasingly on consumers' minds, with 52% of Americans saying they're more worried about being victimized by fraud than normal. 44% of respondents said they've noticed an increase in phone calls and texts from unknown numbers, and emails from unknown sources.

Here are three coronavirus-related online scams to avoid.

Here phishy, phishy
Unsolicited emails that prompt you to click on an attachment should always raise a red flag when you're checking your inbox. But these classic email phishing scams still lure unsuspecting users into downloading malicious items and giving up their login information every day.

With the news that the government is going to issue payments of up to $1,200 in coronavirus relief to US taxpayers in the coming month, the FBI recently issued a warning to be on alert for attackers masquerading as the agency and asking for personal information supposedly in order to receive your check. "While talk of economic stimulus checks has been in the news cycle, government agencies are not sending unsolicited emails seeking your private information in order to send you money," the warning said.

Among other steps to create a safer inbox, the US Cybersecurity and Infrastructure Security Agency recommends turning off your email client's option to automatically download attachments. Not all email clients offer this and each client is different, but some do. Because social engineering attacks -- scams designed to persuade you to hand over your sensitive information by targeting specific information about you -- have become increasingly common in times of crisis, it's also a good idea to read up on how

to identify these security risks.

And remember, never reveal personal or financial information in an email, or respond to requests for it.

Mobile malware
If you're looking to track COVID-19 news with an app, it's a good idea to keep an eye out for malware traps. Earlier in March, a malicious Android app called CovidLock claimed to help users chart the spread of the virus. Instead, it led to a slew of Android phones being locked and held for ransom by hackers.

Researchers at Check Point discovered 16 malicious apps posing as legitimate coronavirus-related apps in a bid to steal users' sensitive data or generate fraudulent revenues from freemium services. Among them, a notorious strain of banking trojan known as Cerberus, which can log all of your keystrokes and let someone command your device remotely.

Meanwhile, Reason Labs recently discovered hackers were using coronavirus-tracking map sites to inject malware into people's browsers. As reported by MarketWatch, coronavirus-related website name registrations are 50% more likely to be from malicious actors.

As Android Authority points out, setting a password on your phone can help protect you from a lock-out attack if you're using Android Nougat. It's also a good idea to stick to the Google Play store for any coronavirus-related apps to better your odds of installing benign software. None of the 16 malicious apps spotted by Check Point were found on an official app store, but were offered on new coronavirus-related websites which the researchers believe were specifically set up to lure new users.

How common are these new coronavirus-related domains? Check Point said it tallied more than 30,103 new coronavirus-related site registrations. 131 of those were considered malicious and 2,777 were "suspicious and under investigation."

Charity checkout
During a disease outbreak or natural disaster, the better angels of our nature compel us to open our wallets to the less fortunate through charitable giving and donation. Before we follow that impulse, we need to take an extra few moments to make sure the charity isn't a funnel into the bank account of a predatory impersonator.

Taking a few moments to review the Federal Trade Commission's Charity Scams page could save you the heartbreak of an emptied checking account. You can also improve your odds by searching sites such as guidestar.org and give.org for the name of your charity before donating.

Source: CNET

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach
- this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Stay tuned for our next lunch and learn date!

www.preferreditgroup.com/beforethebreach

talk nerdy to me

PREFERRED IT EMPLOYEE PODCAST SPOTLIGHT

In April our Director of Operations, Matt Carpenter, was asked to be part of a podcast with The Channel Company to discuss the millennial point of view for working from home during a pandemic.

As you know the COVID-19 pandemic has forced companies and businesses all over the world to make their employees work from home in order to prevent the spread of the virus. This has caused changes for many companies all over our country.

In the podcast, Katie Bavoso, of The Channel Company interviews millennials that all work in the IT field to discuss how things have changed for their companies, how companies are handling the pandemic now, and how to plan for a future pandemic or natural disaster. They also discuss how they feel this pandemic will change the future of remote work, and AI in the world.

Please take a moment to go to https:/bit.ly/3exSE27 to see how this pandemic is changing Preferred IT Group, and other IT companies around the country.

Welcome to the future of Zoom Happy Hours!

We are living in a different type of world right now and we all have had to make adjustments. Social distancing is not always easy. To help with that, many people have turned to virtual social hours with friends and families. Here at Preferred IT, we decided to try this out! We wanted to check in on our team and see how everyone was doing. It is a great experience during this difficult time. Having applications that enable a business to keep the line of communications going are imparative in a time like this. If your company needs help getting set up to work & communicate remotely, give us a call! Cheers from all of us at PTIG!
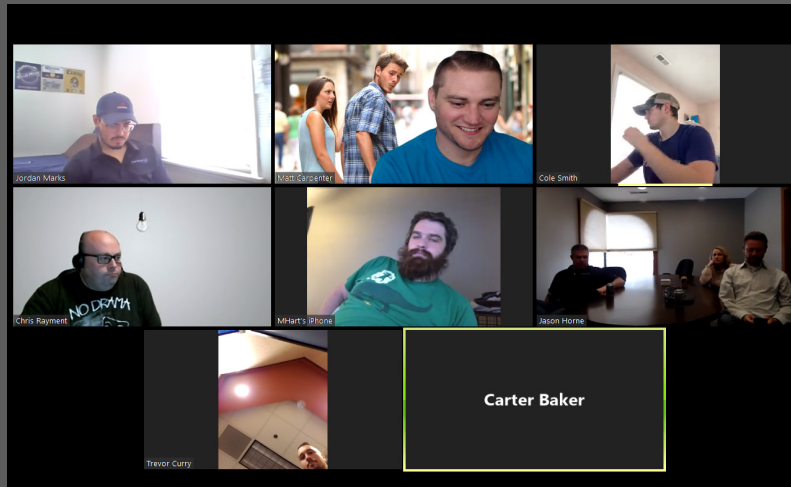
SECURITY TIP!

We don't usually play these, but this looked fun!

Where you are from: STOP
Favorite color: GIVING
First pets name: PEOPLE
Street you grew up on: YOUR
First child's name: PERSONAL
Favorite restaurant: INFO
Favorite teachers name: TO
First job title: GUESS
Favorite food: YOUR
One unpopular opinion you have: PASSWORDS
Favorite singer/band: AND
First type of car you had: SECURITY
Your mother's maiden name: QUESTIONS

preferred group IT

CONTACT US

Fort Wayne
260.440.7377

Warsaw
574.306.4288

Columbia City
260.213.4266

Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.