December 2020

Issue 10 Volume 10

frogworks

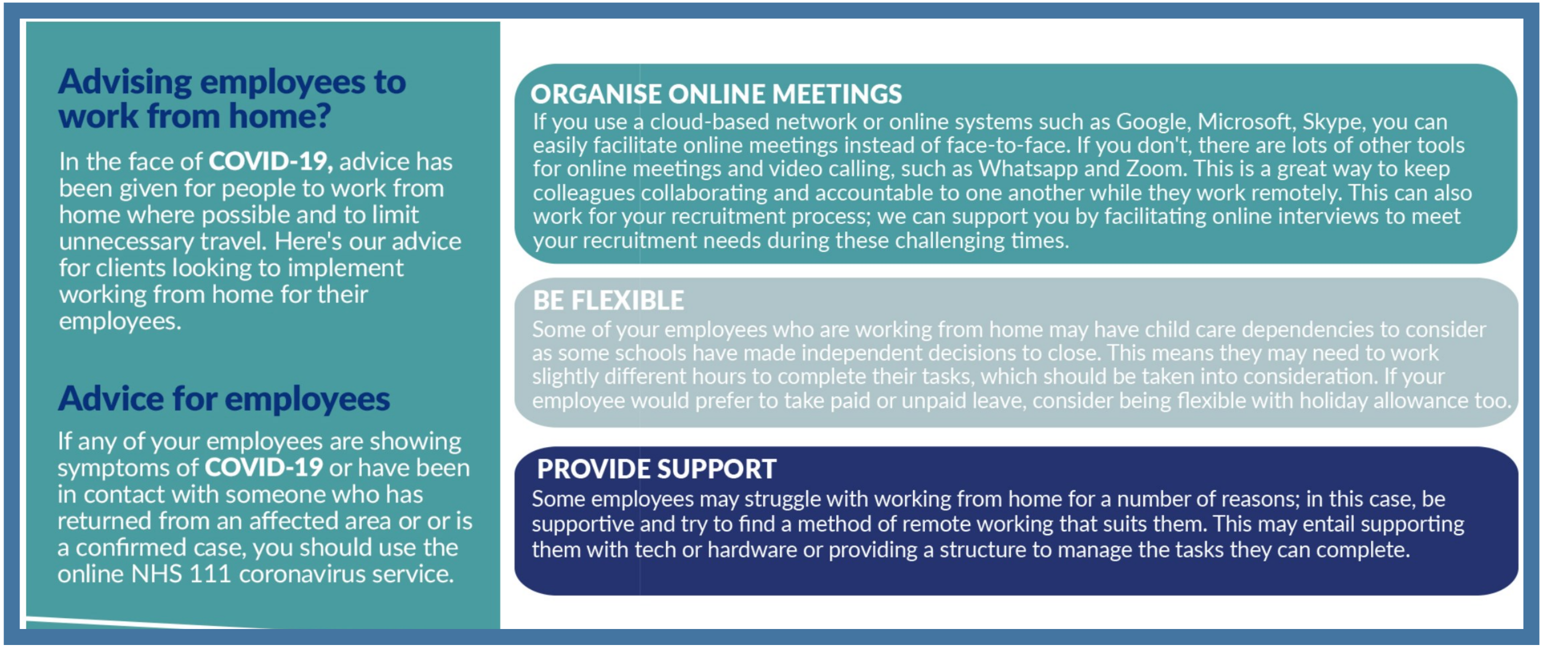
Managing your network so your business doesn't croak.

Run your business without worrying about technology

Ribb"IT" Review

INSIDE THIS ISSUE:

- Remote working advice
- Optimizing Your Working From Home…
- How to Prevent Security Incidents
- How Covid-19 Challenges Privacy



Advising employees to work from home?

In the face of **COVID-19**, advice has been given for people to work from home where possible and to limit unnecessary travel. Here's our advice for clients looking to implement working from home for their employees.

Advice for employees

If any of your employees are showing symptoms of **COVID-19** or have been in contact with someone who has returned from an affected area or or is a confirmed case, you should use the online NHS 111 coronavirus service.

ORGANISE ONLINE MEETINGS

If you use a cloud-based network or online systems such as Google, Microsoft, Skype, you can easily facilitate online meetings instead of face-to-face. If you don't, there are lots of other tools for online meetings and video calling, such as Whatsapp and Zoom. This is a great way to keep colleagues collaborating and accountable to one another while they work remotely. This can also work for your recruitment process; we can support you by facilitating online interviews to meet your recruitment needs during these challenging times.

BE FLEXIBLE

Some of your employees who are working from home may have child care dependencies to consider as some schools have made independent decisions to close. This means they may need to work slightly different hours to complete their tasks, which should be taken into consideration. If your employee would prefer to take paid or unpaid leave, consider being flexible with holiday allowance too.

PROVIDE SUPPORT

Some employees may struggle with working from home for a number of reasons; in this case, be supportive and try to find a method of remote working that suits them. This may entail supporting them with tech or hardware or providing a structure to manage the tasks they can complete.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

> I will honor Christmas in my heart, and try to keep it all the year.
>
> -Charles Dickins

Get More Free Tips, Tools, and Services At Our Web Site: www.GetFrogworks.com
Or call: (240) 880-1944

OPTIMIZING YOUR WFH EXPERIENCE

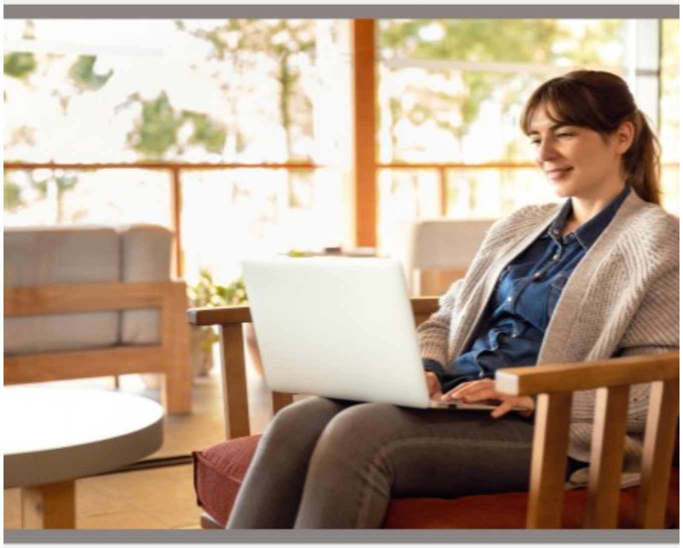
Working from home has been a major adjustment for many. Quite frankly, some love it and some don't. No matter what side you're on, here are some non-technical tips for working remotely.

✓ Find a space with natural light or spend some time during your day outside.

✓ Socialize responsibly. Try communicating with your coworkers through office tools set up by your company.

✓ Create a dedicated workspace where you can focus on performing your tasks.

✓ Stick to your normal working hours, performing work-related tasks during the workday, and save home tasks for after working hours.



✗ Minimize distractions as much as possible during your workday.

✗ Avoid turning on the television, playing games, or browsing the web. It can wait until your break or after the workday is done.

How to Prevent Security Incidents

The truth about incident response plans is that while they're absolutely necessary, we hope to never use them. You can help us by exercising these basic security awareness muscles daily:

Click with caution.

Phishing and smishing (phishing via text message) still hold the top spot on the list of "why data breaches happen." Even when an email appears to come from someone you know (such as your supervisor or co-worker), think before you click, and remain skeptical of any messages that contain random links or attachments.

Use strong, unique passphrases for each account.

A strong passphrase is a group of words that is easy for you to remember but hard for others to guess. And by creating unique passphrases for each account, you prevent criminals from performing an attack known as credential stuffing—the automated use of breached usernames and passwords to gain fraudulent access to additional accounts.

Respect the access you've been given.

Access refers to the digital and physical clearance our organization has granted you. Respect that access by never revealing your login credentials to anyone, by preventing anyone from piggybacking off your badge or keycard, and by ensuring secured areas remain secure.

Limit what you share.

Spear phishing attacks—those that target specific people—often begin with the scammer mining information about their target from public forums such as social media. The more you share with the public, the more potential there is for you to become a target. Consider setting your profiles to fully private, and only connect with people you know in real life.

KNOW THE DIFFERENCE

Security Event vs. Security Incident

An event, according to the National Institute of Standards and Technology, is "any observable occurrence in a system or network." Security events don't always result in breaches (such as a computer crashing), but could still threaten the integrity of an organization's IT infrastructure.

A security incident is a violation of security policies or standard security practices, which results in negative consequences. Incidents can include someone clicking on a phishing link, or a cyber attack that disables our systems and networks.

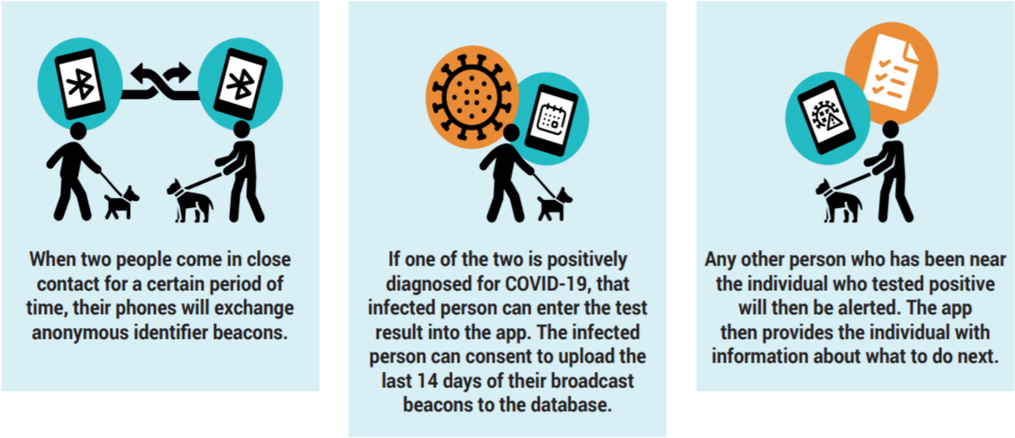
Why does this matter? Our organization encounters events daily. An employee receiving an email registers as an event (the email has cleared our spam filters and firewalls). If it's a phishing attack, it doesn't become an incident until someone clicks! It's your responsibility to ensure events don't become more serious.

How COVID-19 Challenges Privacy

While almost all of us cherish some level of privacy, few of us would sign up for extended periods of social distancing. That, of course, has become the norm since COVID-19 spread worldwide, causing major closures and cancellations.

With that spread came new questions regarding privacy. ***Wouldn't you, for example, want to know if you encountered someone that has or has had the virus? Conversely, would you want others to know if you contracted the virus?*** It's a tricky balance that comes with no easy solutions.

One such solution, as proposed by Apple, Google, and other developers, is an app that notifies you if you came into contact with someone with COVID-19. The app would use *"Bluetooth low energy,"* a feature that allows smartphones to exchange and store anonymous identifier beacons that contain no personal information or location data. Per a white paper released by Google (who partnered with Apple on the project) it would work like this:



When two people come in close contact for a certain period of time, their phones will exchange anonymous identifier beacons.

If one of the two is positively diagnosed for COVID-19, that infected person can enter the test result into the app. The infected person can consent to upload the last 14 days of their broadcast beacons to the database.

Any other person who has been near the individual who tested positive will then be alerted. The app then provides the individual with information about what to do next.

The key to all of this is user consent. It would rely on individuals opting to upload their test results into a central database—a slope that immediately becomes slippery. Could it lead to overreach by data collectors or governments, considering this process essentially amounts to surveillance? How long does the data stay on the server, and when will it be deleted? Can users opt out and reverse consent? If you got sick, would you give consent for a third party to harvest this data?

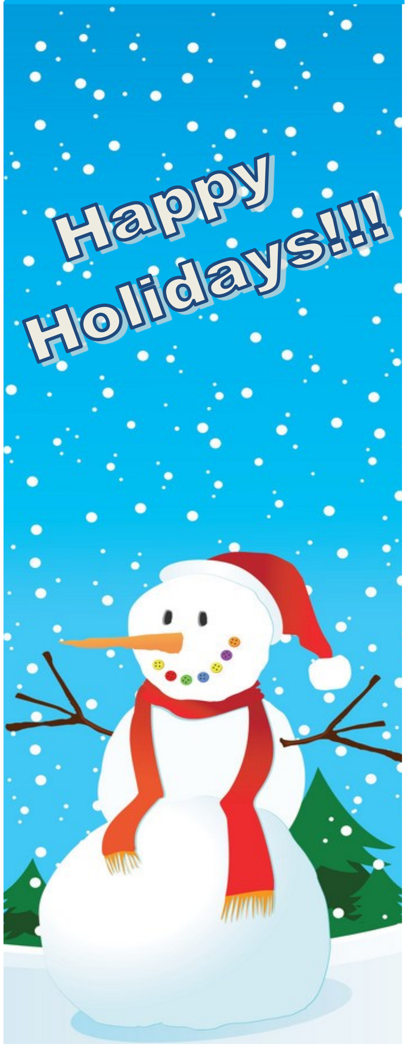
Extraordinary situations call for extraordinary measures, to be sure. The COVID-19 pandemic illustrates the incredibly thin line that separates the right to privacy versus the need for data collection, especially where public health is concerned. When it's all said and done, COVID-19 may change the way we handle protected health information in the future.

@ The Security Awareness Company, LLC

Thank you for all of your support In 2020. We wish you a peaceful and wonderful holiday from your friends at:

frogworks

Managing your network so your business doesn't croak.



We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

and sign up.

BBB ACCREDITED BUSINESS

We are excited and proud to announce that Frogworks has been accredited by the Better Business Bureau!

WE'VE MOVED!

2670 Crain Highway, Suite 304
Waldorf, MD 20601

Get More Free Tips, Tools, and Services At Our Web Site: www.GetFrogworks.com
Or call: (240) 880-1944