HAPPY★NEW★YEAR

frogworks

Managing your network so your business doesn't croak.

January 2021

Issue 1 Volume 11

Run your business without worrying about technology

Ribb"IT" Review

INSIDE THIS ISSUE:

New Year-Remote Work is Here to Stay!

If you must adopt a work from home lifestyle, set yourself up for success by creating a dedicated and comfortable space that is free from distractions.

Keep the physical security of devices as a top priority when taking equipment to and from the office. Minimize pit-stops and protect devices with encryption if possible.

Be on the lookout for any COVID-19 related texting and phishing scams that are currently rampant.

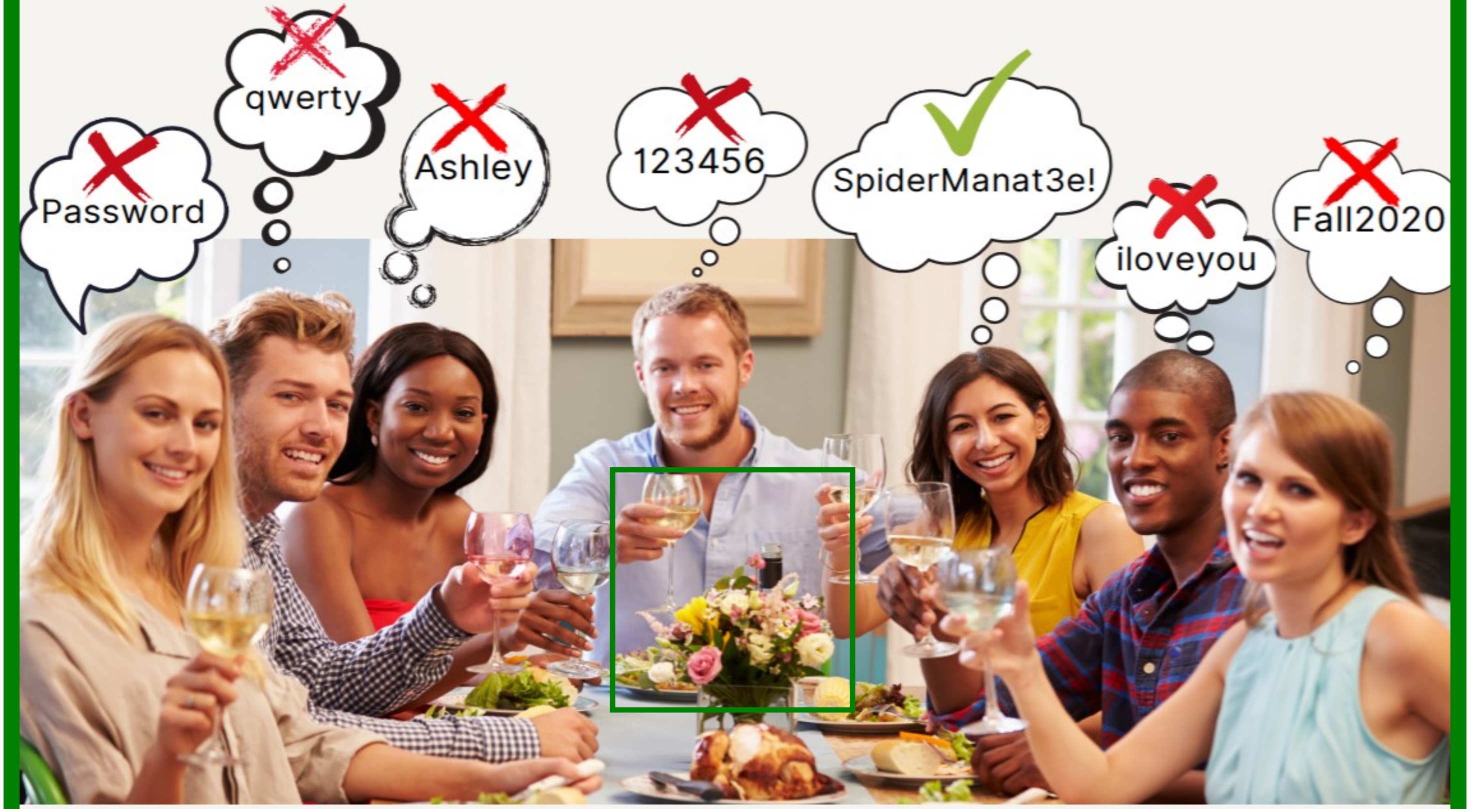
This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

> 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

The Password Paradox

Breaches can be very revealing for those involved, and the passwords exposed truly illustrate risky user behavior. Using our Dark Web insight, it's clear to see many of us are still using and reusing weak passwords. So think hard about all of ***your*** passwords... are they strong enough to keep your accounts safe?



So, how can we set up strong and unique passwords across all of our accounts? Technology can help! A password manager can help create and manage your passwords, while two-factor authentication can add an extra layer of security.

PASSWORD MANAGER BENEFITS

No more CREATING passwords

No more CHANGING passwords

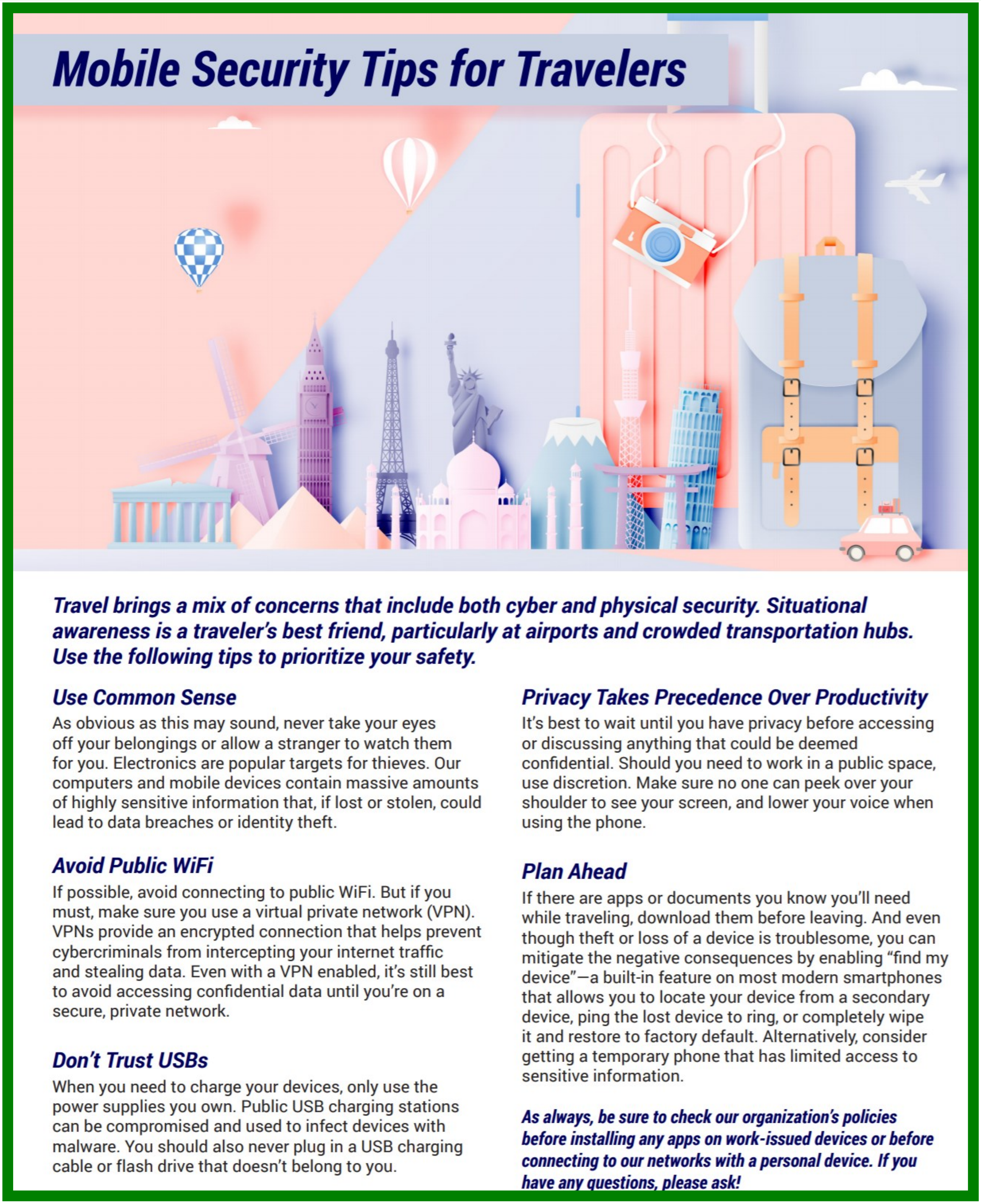
Only need to remember ONE password

Inexpensive or sometimes FREE to use

A large suite of SECURITY features to keep your accounts and passwords safe

Tip

For added security, enable **Two Factor Authentication** wherever possible. Start with critical accounts like banking, financial, and any work-related sites where sensitive data is accessed.



Mobile Security Tips for Travelers

Travel brings a mix of concerns that include both cyber and physical security. Situational awareness is a traveler's best friend, particularly at airports and crowded transportation hubs. Use the following tips to prioritize your safety.

Use Common Sense

As obvious as this may sound, never take your eyes off your belongings or allow a stranger to watch them for you. Electronics are popular targets for thieves. Our computers and mobile devices contain massive amounts of highly sensitive information that, if lost or stolen, could lead to data breaches or identity theft.

Avoid Public WiFi

If possible, avoid connecting to public WiFi. But if you must, make sure you use a virtual private network (VPN). VPNs provide an encrypted connection that helps prevent cybercriminals from intercepting your internet traffic and stealing data. Even with a VPN enabled, it's still best to avoid accessing confidential data until you're on a secure, private network.

Don't Trust USBs

When you need to charge your devices, only use the power supplies you own. Public USB charging stations can be compromised and used to infect devices with malware. You should also never plug in a USB charging cable or flash drive that doesn't belong to you.

Privacy Takes Precedence Over Productivity

It's best to wait until you have privacy before accessing or discussing anything that could be deemed confidential. Should you need to work in a public space, use discretion. Make sure no one can peek over your shoulder to see your screen, and lower your voice when using the phone.

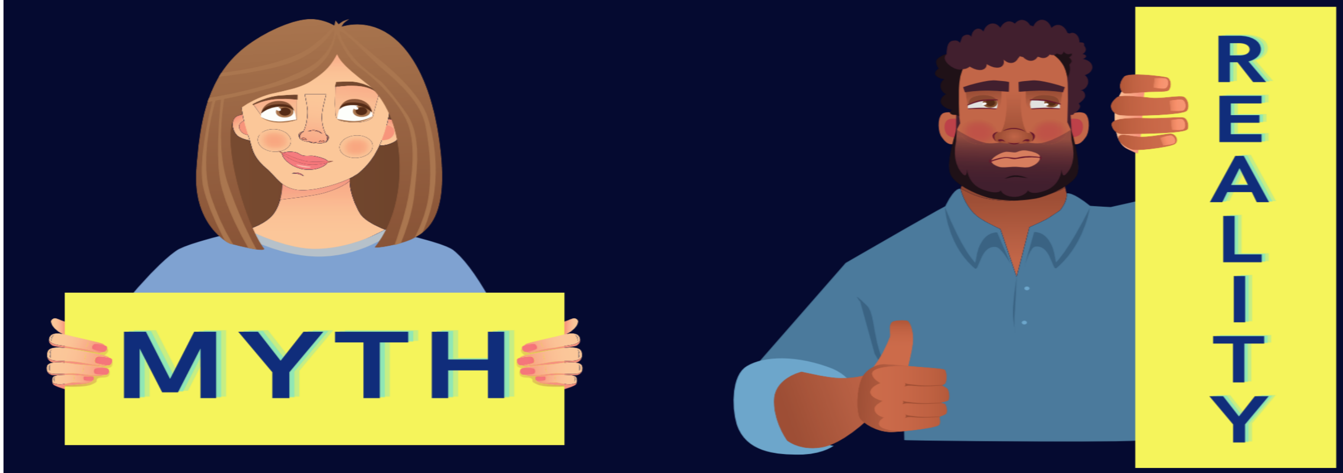
Plan Ahead

If there are apps or documents you know you'll need while traveling, download them before leaving. And even though theft or loss of a device is troublesome, you can mitigate the negative consequences by enabling "find my device"—a built-in feature on most modern smartphones that allows you to locate your device from a secondary device, ping the lost device to ring, or completely wipe it and restore to factory default. Alternatively, consider getting a temporary phone that has limited access to sensitive information.

As always, be sure to check our organization's policies before installing any apps on work-issued devices or before connecting to our networks with a personal device. If you have any questions, please ask!

Top Cybersecurity Myths

Cybersecurity can be a tough subject to master. To help, let's examine some of the common misconceptions that need to be debunked.



Small & medium-sized businesses aren't targeted by cybercriminals.	A majority of data breaches happen at small businesses. Often, small and medium-sized businesses lack the proper security measures and training to defend against cybercriminals, making them a major target.
A strong password alone will protect your accounts.	A strong password is important, but there are other steps that can also enhance your security. Multi-factor authentication will help protect your account a step further, along with many other necessary security measures.
I was found on the Dark Web from a breach a few years ago, so what!?	Any time your information is found on the Dark Web it should be taken seriously. Personal information on the Dark Web can be used for sophisticated phishing emails and you may still be using those old login credentials elsewhere.

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