1127 International Parkway, Room 249
Fredericksburg, VA 22406
(540) 446-9322

SECURITY NEWSLETTER JANUARY 2020

FOR MORE INFORMATION ABOUT SECURITY AWARENESS VISIT:

https://www.sans.org/security-awareness-training

ACKS

ness

a common risk of working remotely
s having to connect to and work
points. These points might be the
el, airport, or local coffee shop. But
c networks? Who could be watching
doing online? While a shared or
incredibly convenient while on the
exposing your personal data and

haviors to reduce that risk of data
ng and accessing public Wi-Fi.

r browsers and plugins always have
zing ways to detect new
ly patching it. Current and updated
on't ignore those system update
of the simplest ways to ensure your

sions, be sure to check your
ized. If you are unsure, simply ask

Encryption is a technology that helps protect your information when transmitted over the Internet. When you connect to public Wi-Fi points, you want to be sure all of your activity online is encrypted, ensuring others cannot monitor or capture what you do online. For example, when you're browsing the web, you want to ensure your browser is connected to websites that are encrypted. Not sure if your browser connection is encrypted? Look to the top of your browser. If you see a padlock or HTTPS next to the website address, this is an indicator that your connection to the website is encrypted.

WBSI
ISO 9001:2015 web business solutions inc.

1127 International Parkway, Room 249
Fredericksburg, VA 22406
(540) 446-9322

One of the simplest and most effective ways to encrypt all of your online activity is to use a Virtual Private Network (VPN). The technology behind a VPN creates a private, encrypted tunnel for your online activity, therefore making it much more difficult for anyone to watch or monitor your online activities. A VPN can also help hide your location, which makes it much more difficult for the websites you're visiting to determine your precise location.

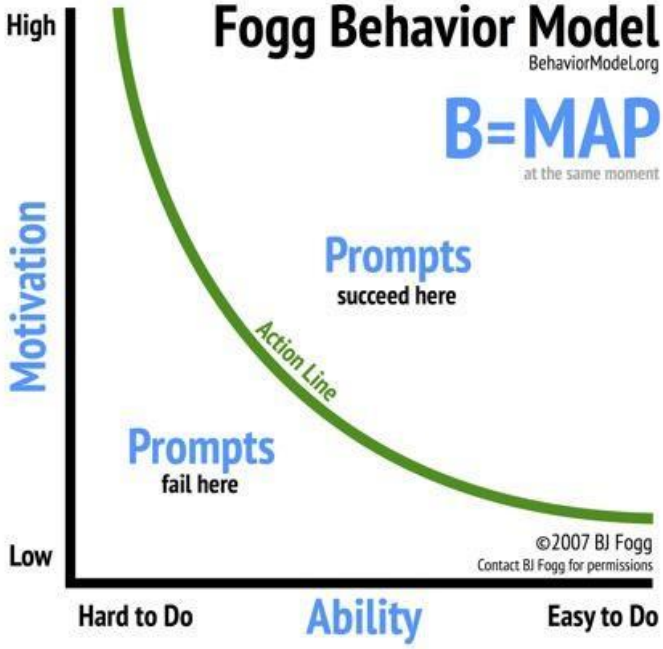
Tethering

Wi-Fi tethering, also known as a mobile hotspot, refers to the action of connecting one device, such as a smartphone or a tablet, to another, such as a laptop, so that you may share the internet connection between devices when a Wi-Fi connection is unavailable. When in doubt about the security of a public Wi-Fi network, it is good practice to tether your network connection off of your smartphone instead of using the public Wi-Fi.

While this may not always be possible, especially when traveling internationally, it is one of the most secure methods to connect to Wi-Fi while traveling.

Yourself

Ultimately **you** are the best defense. If something about the Wi-Fi connection seems odd or suspicious, simply don't connect. Find another Wi-Fi network you feel more comfortable with or tether from your mobile device. In addition, many of today's online attacks are not targeting your technology but attempting to trick or fool you. If you receive an email, message, or phone call that seems odd or suspicious especially highly urgent ones, it may be an attack. Always be on alert.



Try to remember: Engage people with actionable behaviors that they can truly exhibit. A wonderful model to help you understand the science behind behavior change is the BJ Fogg Behavior Model. This model indicates that three elements must touch at the same moment for a specific behavior to occur: Motivation, Ability, and a Prompt. When a behavior does not occur, it is the belief that at least one of those three elements is missing. Are you motivated to change behavior? Do you have the ability to change your behavior? Are you prompted to change your behavior?

1127 International Parkway, Room 249
Fredericksburg, VA 22406
(540) 446-9322

It is unreasonable to tell people in the workplace to *never* use public Wi-Fi. And smacking them down with an overwhelming list of detailed steps to stay secure is not only impractical, but it can also have a negative impact on workplace productivity and data security. The goal is to manage your human risk by enabling people to secure themselves in ways anyone can follow. Next time you're traveling and need to connect to Wi-Fi, try to keep these four simple key behaviors in mind. Your data and your company will thank you.

Any Questions? Please contact us:

Holly Higgins/FSO: holly.higgins@wbsi.com

John Deffenbaugh/AFSO: John.Deffenbaugh@wbsi.com

Sarah Del Cid/AFSO: Sarahk@wbsi.com