10TH ANNIVERSARY

IT Radix Resource

We make IT work for you

Fall 2018

Only YOU Can Prevent Online Threats

National Parks are wonderful, except when they are not—just like when you are visiting all sorts of websites online. In both cases, staying safe and ensuring your security, should be the top priority. Here are some tips to keep you safe in both environments:

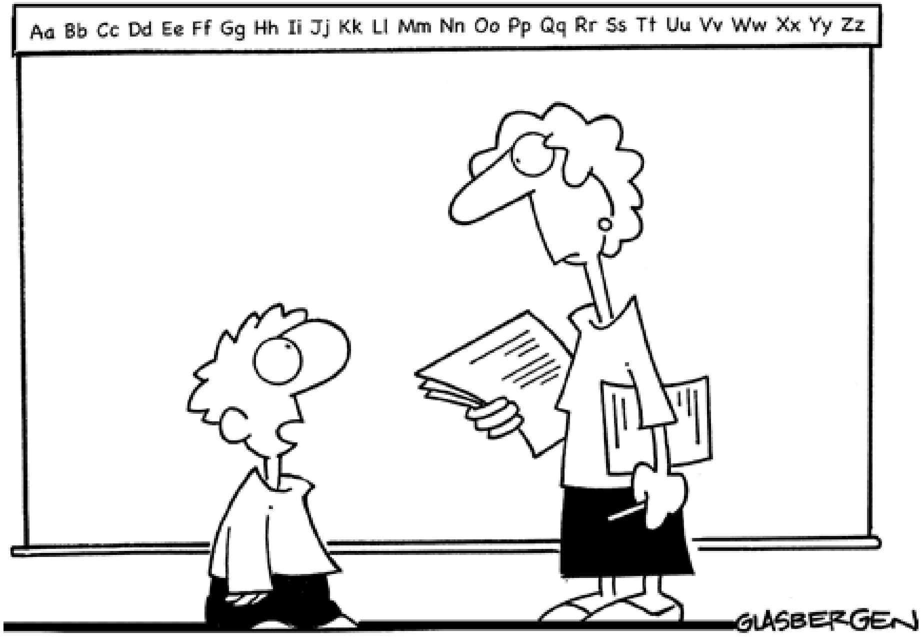
"Go" Before You Go — Your mother told you, so we do not mind reinforcing it! Public bathrooms can be dens of bacteria and yuck, especially in National Parks with so many visitors. It is not easy for the Park Service to keep them clean. Try to avoid them at all cost. Likewise, avoid using public computers and public Wi-Fi whenever possible—each increase your odds of infection.

Lock Your Doors — Surely all the other visitors in the parking lot are nice people on vacation enjoying the park just like you, NOT! So be careful—lock your car doors when you leave it and secure your valuables wherever you go. The same is true when on any technology device or website, be sure you use strong passwords and change them frequently!

Stay on the Trail — While "venturing off" may seem enticing while hiking through some beautiful landscape, it is not without risk. So too when online, be careful and avoid clicking on some "bait" that might take you to a risky place. Connect securely over https (not http). Note that the "s" stands for "secure."

Leave Wildlife Alone — There is a reason they are called wildlife. Leave them alone. Internet wildlife can be just as frightening when it is near. So, stay away from it all. Use a web filtering firewall and employ real time URL checking to provide a defense.

Wear Sunscreen — A National Park visit almost always means you are outside, so protect yourself with sunscreen to reduce exposure to the negative effects of the sun. And anytime you are working on a PC, especially when online, ensure that you have the latest protection which includes installing the latest updates for your PC and using an updated anti-virus 100% of the time.


Aa Bb Cc Dd Ee Ff Gg Hh Ii Jj Kk Ll Mm Nn Oo Pp Qq Rr Ss Tt Uu Vv Ww Xx Yy Zz
GLASBERGEN

"Yes, I copied off Norman's paper. Is it my fault if information security is lax around here?"

Don't Touch — The best advice in any park setting is to leave natural objects alone. In fact, everything in a National Park is federally protected and should remain in the park. Likewise, when online, be careful where you click and practice "click economy." Careless clicking can lead you to touch the online version of poison ivy…or far worse!

Keep Up Your Guard — Always be cautious in our park system; you really do not know the area very well nor do you know the people around you, so keep up your guard. Take all preventative measures when online as well, such as using anti-virus software, employing a firewall, and being careful with whom you share anything.

Clean Up — Just as leaving food debris around a campsite is an invitation to a visit from hungry wildlife, so too is not cleaning your cache on any computer or device. All browsers on any device typically keep track of where you have been and what you have done. It is easy for outsiders to view that cache, so set your preferences not to record any of your online activity.

Some might fear a bear attack in a national park. The same individual might also fear a direct strike into their computer from an outside attacker. But the truth is that in both National Parks and in surfing the web, most injuries that occur are self-inflicted often due to lack of preparedness or awareness. Follow these tips and stay safe! The words of Smokey Bear pertain to both staying safe in the woods AND online, "Remember…only YOU can prevent forest fires" (or online threats).

Why So Many Passwords?

Thinking up passwords and managing them is a big pain, no two ways around it. One website requires a symbol, and another requires 14 characters. Meanwhile, your bank requires 10 characters, four PIN numbers and the answer to a secret question. In the midst of all this, it's easy to just use the same three or four passwords for everything—after all, that's more secure than a single password, right?

But imagine this... Say you use the same password for your Gmail, your Amazon and the account you use to order gift cards at a 10% discount for client gifts. One day, the gift card website is hacked. Not only do the crooks get your credit card info, they also get the list of all the website's users and those users' passwords. Then, they publish these freely on the Internet's Dark Web. But if you use different passwords for all your accounts, you're safe despite any crisis that may arise. Make sure you practice good password security.

National Park Fun Facts!

- The national parks are habitat for more than 400 endangered or threatened plant and animal species.
- The Grand Canyon is known as one of the *Seven Natural Wonders of the World*.
- Mesa Verde was the first national park to be recognized for "works of man," an acknowledgement of the incredible cliff dwellings left behind by the Pueblo Indians.
- The smallest national park unit is part of an acre in downtown Philadelphia, the Thaddeus Kosciuszko National Memorial.

The "Not Me" Problem

Security this, password that! Now they want a password with 14 characters and 2 symbols? And I must change it every three months?

As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code—you get the idea. But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

> "We travel not to escape life, but for life not to escape us."
>
> — Anonymous

Kids Careless with Online Passwords

With corporations taking hits left and right from cybercriminals, security on the Internet has become more important than ever. Still, even as many of us step up the security of our online presence, stragglers who believe they're immune to such attacks abound.

Based on a recent survey from Statista, young people are more careless with passwords. Thirty-four percent of people aged 18 to 34 years use the same password for "most online logins," compared to only 20% of the 35 to 54 demographics, and only 13% for those older than 55. In addition, a whopping 10% of 18- to 34-year-olds use the same password for all their online keys.

It goes without saying that this is bad practice. It can be all too easy to hack into a single, less secure account. However, if different passwords are used for separate logins, it becomes much more difficult to access more important files in, say, a Gmail account or bank login. Not so if the passwords are identical.

BusinessInsider.com 10/18/2017

Did We WOW You?

Let us know…

www.it-radix.com/wow-award