The Beacon

Florida Fusion Center #17-060 | Cyber and Critical Infrastructure Report | April 2017 Issue #13

Summary

Car Hacking: The Dangers and Realities - In theory, anything with a computer can be hacked…including cars. But the risk of that happening is unlikely.

Show Me the Money: Person-to-Person Payment Apps - Transferring money to others is easier than ever with these apps. This article covers some security concerns that go along with them.

The Risks with Ride-Sharing - These types of apps are extremely convenient, but is there a privacy price to be paid?

Are Your Devices Spying on You? - Smart devices that can record you are handy for enhancing the user experience, but may be compromising your security.

Traveling Safely with Your Device - We are all tethered to our devices, even when we travel. Here are some tips to keep in mind to ensure their security before, during, and after your travels.

Working With Transparency - Even if it looks like the background of an image is empty, it's really made up of pixels—and even those can be exploited by hackers.

Contents

About *The Secure Florida Beacon*

The Secure Florida Beacon is published by Secure Florida to highlight cyber and critical infrastructure security information and awareness. Secure Florida is an internet safety and awareness effort of the Florida Department of Law Enforcement's Florida Infrastructure Protection Center (FIPC).

The Florida Infrastructure Protection Center (FIPC) was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters.

Contact Secure Florida at:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Editor's Corner

Hacking Your Privacy

In recent weeks, there have been many headlines about a leak of a large volume of Central Intelligence Agency (CIA) documents. Allegedly, these documents contain tactics for electronic surveillance efforts, including how to circumvent the encryption of messaging apps like Signal, or hack into smart TVs to listen in on private conversations. If the CIA can hack into these devices (and then if these leaked documents provide common cyber criminals a blueprint to do so as well), is all hope for privacy lost? Fear not, dear Beacon readers, for the dangers associated with this latest news can mostly be mitigated simply by employing some best practices for computer and Internet security.

Cracked Encryption?

Many reports say that the CIA has cracked the encryption for some widely-used apps. Whether it's the CIA, terrorists, or simply common criminals who are trying to eavesdrop, compromised encryption is a concern. It likely isn't the case that encryption has been cracked, however. Instead, it mostly comes down to social engineering.

The best way for any hacker to get access to your device is to exploit an outdated operating system or application. They need to find a way to get to your device, and that probably involves sending you malware, often through a malicious link. Once your device is compromised, then encryption no longer matters; if they have access, a hacker can see everything on your device.

What can your Smart TV hear?

Some other headlines have said that smart TVs can be manipulated to spy on you: hackers can get access and covertly turn on a microphone or camera. But this is nothing new—this vulnerability has been widely reported for a few years. According to Samsung's SmartTV privacy policy, users should "be aware that if your spoken words include personal or sensitive information, that information will be among the data captured and transmitted to a third party."[1]

Any type of computer can be hacked, and anyone can be socially engineered. However, employing some best practices goes a long way to helping insure against these risks. As a reminder:

1. Keep all of your software up to date (and on mobile devices, delete any apps you don't need).
2. Make sure to have long, strong, unique passwords.
3. Never click on suspicious links.
4. Avoid connecting to unsecured Wi-Fi.

For more information on how to protect your devices, check out **Are Your Devices Spying on You?** on page 9.

[1] http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/

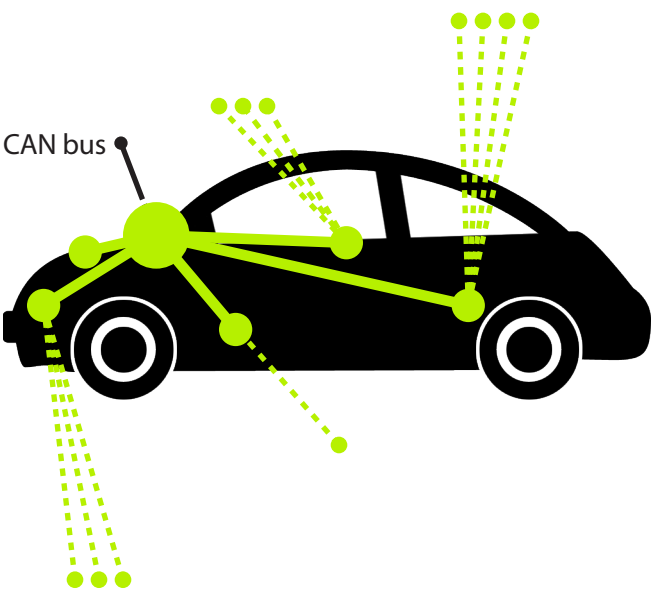
Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Cyber Threats

Car Hacking: The Dangers and Realities

Computers are heavily integrated into our daily life, but sometimes people forget how much they are integrated into the vehicles we drive every day. We have computers running more code in a modern high-end vehicle than a 787 Boeing passenger plane.[1] Code can be manipulated in a desktop computer to make it perform malicious actions, so why not do the same in cars?

In 2015, security researchers Charlie Miller and Chris Valasek remotely hacked into an unaltered 2014 Jeep Cherokee. They were able to remotely manipulate some functions of the car, such as turning the radio on full volume or spraying windshield wiper fluid, by exploiting security holes left by the vehicle's manufacturer.[2] Although something like manipulating radio volume is a minor annoyance, the darker side of their testing revealed they could also control the throttle, slam on the brakes, or even turn the steering wheel.



This graphic, a simplified version of one found in a SANS Institute paper (https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607) illustrates how the CAN bus and its components work. The CAN bus, the large green dot, communicates with various aspects of the car, represented by the smaller green dots. Some of these components, such as the radio or the keyless entry hub, additionally communicate with things outside the car's internal communication line, like your iPhone for music and your keys to get in the car. These outside communication lines, the dotted lines, are the vulnerable lines hackers can attempt to take advantage of.

These attacks happen through the manipulation of messages sent to the Controller Area Network bus, or the CAN bus, developed in the 1980s. Before the CAN bus, vehicle components that needed to communicate needed a direct connection, which increased the needed wiring. The CAN bus eliminated the need for the direct wiring connections by managing different component operations such as the windows, engine, or transmission.[3] Data is constantly sent and distributed from the CAN bus, and that is where hackers come in. They can send spoofed data streams to the CAN bus system, making it do things the driver may not want (like slam on the brakes). Because this system was developed in the 1980s (remember the Internet we know today was nonexistent) they were not expecting people to hack these systems, so security like data encryption or having firewalls was not a consideration in the design.

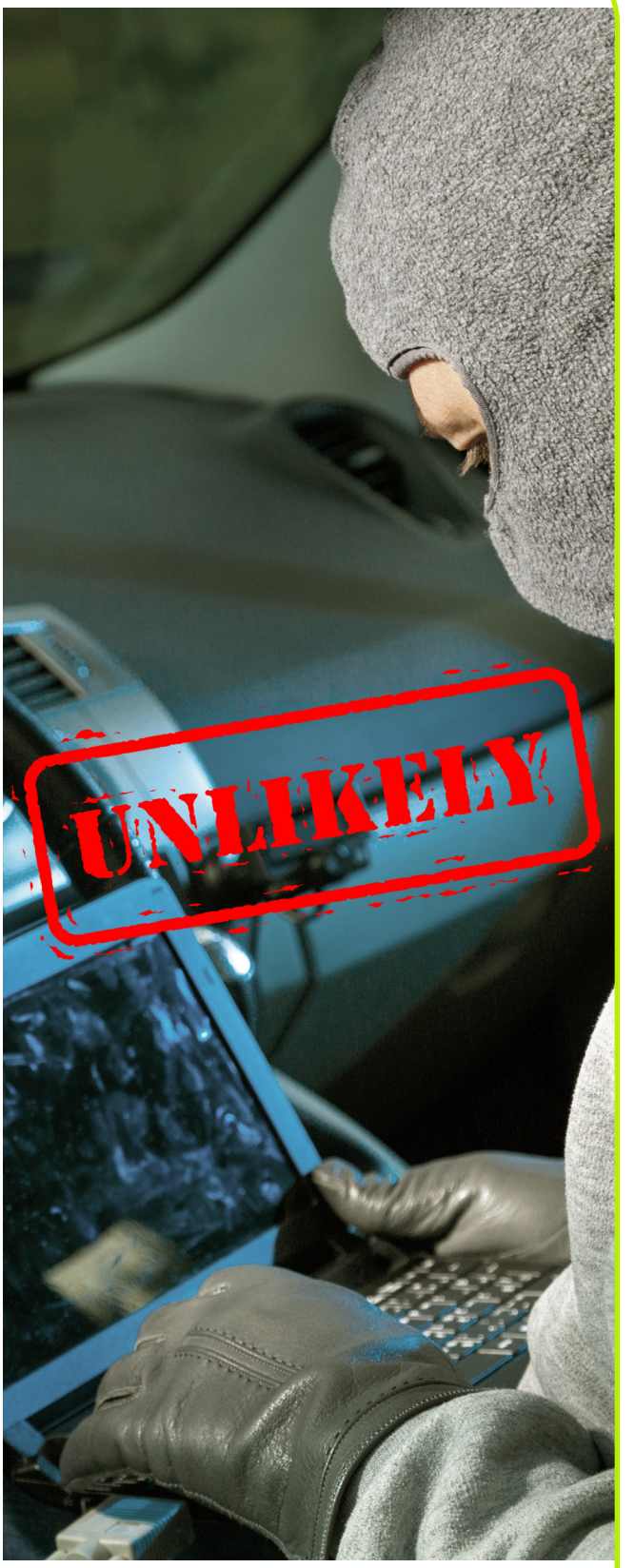
[1] https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607
[2] Ibid.
[3] Ibid.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

How does this affect you? Well, you shouldn't be worried about some hot-headed teenagers hacking into your vehicle and causing damage. Hacking into a vehicle requires extensive research into the CAN bus. Miller and Valasek have a lot of experience hacking vehicles; before the 2015 project, they were granted $80,000 by the Defense Advanced Research Projects Agency (commonly known as DARPA) to find security vulnerabilities in vehicles and published their findings in a 2014 research paper.[4] You don't have to worry about any common criminal hacking your vehicle either. It's good news that these researchers hacked into cars first as white hat hackers (hackers contracted to hack something so they can find vulnerabilities in a system) rather than black hat hackers (hackers who hack for malicious intent).

Because Miller and Valasek published their findings, car companies were forced to address the issues. For example, Fiat Chrysler Automobiles recalled 1.4 million vehicles for a critical security update.[5] Miller and Valasek wrote another research paper on the Jeep Cherokee hack in 2015, explaining that the vehicles' Bluetooth or Wi-Fi capabilities were the most likely attack vectors that malicious actors could exploit.[6]

At the end of the day, however, you shouldn't have to worry about your car being hacked as you drive home today. Any vehicle hacking currently requires a plethora of knowledge and money. If researchers like Miller and Valasek continue their work, car manufacturers should patch vehicle vulnerabilities they discover. In the long term, the main goal is for manufacturers to start making vehicles with computer security in mind, rather than patching it later. The day that happens, car hacking will become an even smaller risk.



[4] http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
[5] https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607
[6] http://illmatics.com/Remote%20Car%20Hacking.pdf

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Cyber Highlights

P2P Payment Service Apps

Today, we can access so many things instantly with just a couple swipes on a mobile device. It only makes sense, then, that there should be a way to instantly give someone money without the hassle of carrying cash.

With P2P (person-to-person) payment apps, the idea is that you can use a mobile application to seamlessly transfer money to another individual: the babysitter, your roommate for your share of rent, or to split the lunch tab. Funds are transferred in-app between user accounts. Once the transaction is final, the funds can be transferred from the app directly into a bank account, or users can keep the funds in their app's account to use for future transfers. Depending on which P2P payment app you use, the process from the initial in-app payment to transferring the funds out of the app and into a bank account takes from one to three business days.

Although these apps, in theory, make the process painless to settle your debts (large or small) without needing to carry a checkbook or cash, there are some security concerns to keep in mind when using P2P payment apps.

What are the risks?

P2P payment apps do guarantee security protections such as encryption and enhanced authentication features (like a PIN). Some, but not all, have FDIC insurance for deposits held in-app.[1] However, these security features are not a surefire way to guarantee the safety and security of your account. One Venmo user discovered his account had been hijacked, because someone discovered his password. The hacker logged in, changed the email address and password, and proceeded to transfer $2,850 from the bank account linked as his primary payment method.[2]

Many of the user agreements for these apps do not have buyer or seller protections, which may leave you open to a scam, should you transact with someone you don't know. One app user reported that they sold basketball tickets to a stranger, only to discover the transaction was reversed for insufficient funds…after they had already sent the tickets to the buyer.[3]

[1] http://www.digitaltrends.com/mobile/paypal-vs-google-wallet-vs-venmo-vs-square-cash/
[2] http://www.slate.com/articles/technology/safety_net/2015/02/venmo_security_it_s_not_as_strong_as_the_company_wants_you_to_think.single.html
[3] http://www.slate.com/articles/business/moneybox/2015/09/venmo_scam_and_fraud_why_it_s_easy_to_get_ripped_off_through_the_mobile.html

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Where's the money coming from?

More specifically, what traditional payment method (debit card, credit card, or bank account information) should you link to your app so that you can actually use it to send or receive funds? We recommend always using a credit card, because it is an added protection against fraud: credit card companies are required by law to provide certain protections to consumers in the event of fraudulent activity.[4] However, if you link a debit card or checking account, you run the risk of losing your money forever if you become a victim of a scam (as in the examples above). Most P2P payment apps do assess a transaction fee if you use a credit card, usually 2-3%, which is a small price to pay to keep your bank account safe.

Keep in mind that some P2P apps have better security features than others. Poor quality security protections may mean that it is as easy for a criminal to hijack your account as it is to pay your friend back for buying you that burger the other day. It is important to weigh carefully the tradeoff between convenience and security. The chart below compares some popular P2P payment apps and their features.

	Transaction Limits (per)	Security Features	Payment Method	Special Features
Circle[5]	None*	• FDIC insured • Touch ID, PIN codes	Credit, Debit, Bank Transfer	Can send money between US dollars, GB pound, and Euro
Paypal[6]	$10,000	PayPal Purchase Protection	Credit, Debit, Bank Transfer	Can create personal PayPal links, which enable direct payment
Google Wallet[7]	$9,999	24/7 fraud monitoring covers 100% verified unauthorized transactions	Credit, Debit, Bank Transfer	Syncs with other Google services
Venmo[8]	$3,000	Enables Touch ID, PIN code	Credit, Debit, Bank Transfer	Social media integration (Facebook)
Square Cash[9]	$2,500	• FDIC insured • **No** password/ PIN authentication	Credit, Debit	Social media integration (Snapchat)

* There is no limit on transfers within Circle. Circle initially restricts users to adding $400 into their Circle account per week from their card/bank account, but users can request an increase (up to $3,000) based on eligibility.

[4] https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges
[5] https://www.circle.com/en
[6] https://www.paypal.com/us/home
[7] https://www.google.com/wallet/
[8] https://venmo.com/
[9] https://cash.me/

The Risks of Ride Sharing

There is no denying the benefits produced by ride sharing technologies over the past several years. Organizations such as Uber and Lyft grant consumers the capability to request car transportation, and even food delivery, in more than 500 cities worldwide through the convenience of a mobile application. However, recent open source reporting has brought a number of allegations to light surrounding the legality of how Uber obtains and uses data of its customer base.

Greyball is the name of an internal tool developed by Uber that uses data collected from the Uber app to identify and circumvent targeted individuals, particularly government officials. In 2014, the company used Greyball to target city inspectors in Portland, Oregon who were posing as regular customers to covertly gather information to prove that Uber was operating illegally. These individuals were then flagged ("greyballed") by Uber. This meant that when these users attempted to request a ride, the service showed them fake versions of the Uber app, complete with fake drivers.[1] Any Uber drivers who actually had agreed to give these officials a ride would cancel the transaction upon learning their greyballed status, sometimes at the direction of Uber. How did Uber know that these "customers" were in fact city officials? According to the New York Times, one technique Uber implemented was to draw a digital perimeter, or "geofence," around government offices on a digital map of a city where Uber operated. The company watched which people were frequently opening and closing the app in these geofenced areas, or reviewed a user's credit card information to determine if the card was associated with an institution that would indicate they were government employees, such as a police credit union.[2]

[1] http://www.denverpost.com/2017/03/03/bad-news-for-uber/
[2] https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html?_r=0

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Uber reportedly used over a dozen techniques to assess whether users were regular riders or possibly government officials.[3] Uber tagged greyballed accounts with a small piece of code that read "Greyball" followed by a string of numbers.[4] While Uber has stated that the purpose of the program is to "[deny] ride requests to fraudulent users who are violating our terms of service, whether that's people aiming to physically harm drivers, competitors looking to disrupt our operations, or opponents who collude with officials on secret 'stings' meant to entrap drivers,"[5] there are a number of issues with the legality of this statement. The most notable issue is that government-sanctioned 'stings' are typically well within the course of the law and an essential duty for a number of law enforcement or regulatory agencies. The legal battle in Portland, Oregon has spilled over into other regions within the United States including Florida, specifically Hillsborough County.

In response to the *New York Times* report on Uber's Greyball program, Uber issued a statement on March 8, 2017 formally admitting the use of the tool to thwart city regulators and to announce a review of the technology.[6] Uber's chief security officer, Joe Sullivan, wrote, "We are expressly prohibiting its use to target action by local regulators going forward."[7] It will undoubtedly take time for these changes to go into effect, but this series of revelations over the past several weeks has brought to light what many recognize as the dark underbelly of ride sharing. When we use these types of apps, there is a lot of information we hand over about ourselves. It is important to remember that while these services may be convenient, you might not know how the personal information you're sharing is being used.

[3] https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html?_r=0
[4] https://www.nytimes.com/2017/03/03/technology/uber-greyball-program-evade-authorities.html?_r=0
[5] http://www.denverpost.com/2017/03/03/bad-news-for-uber/
[6] http://www.usatoday.com/story/tech/talkingtech/2017/03/08/uber-stop-using-greyball-target-regulators/98930282/
[7] https://newsroom.uber.com/an-update-on-greyballing/

Are Your Devices Spying on You?

You never know who's listening…or watching, for that matter. Many of the smart devices, increasingly used worldwide, contain cameras, global positioning system chips, or always-listening microphones. Or all three. Who might be listening, watching, or possibly recording, and should we be concerned?

Samsung SmartTVs,[1] personal assistant devices like the Amazon Echo and Google Home,[2] and other Internet of Things (IoT) devices can be incredibly helpful, but they also contain the potential for unforeseen risks. Samsung Smart TVs have been in the news as far back as 2015, when researchers noticed that voice recognition data from people's homes was being sent to a third party for analysis—even if they had opted out of voice recognition.[3] Recently, news outlets have also purported that intelligence agencies have researched how to hack Samsung Smart TVs for covert

[1] http://www.samsung.com/sa_en/tvs/overview/smart/
[2] https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E
[3] http://money.cnn.com/2015/02/09/technology/security/samsung-smart-tv-privacy/

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

surveillance purposes.[4]

Personal assistant devices like Google Home[5] and Amazon Echo pose some interesting risks: they are always on, always listening, and always potentially recording audio (or video, based on the type of device). Personal assistant devices respond to key or "wake" words that allow you to talk to the device to ask questions, order items, set calendar events, and in some cases control other smart devices (like your home's thermostat). In an effort to make things easier for the user, the devices afford almost complete access to personal data. However, here are some unintended consequences consumers have experienced:

- During the Super Bowl, a commercial aired using the Google Home device activation command, triggering thousands of devices in homes airing the game.[6]
- A TV news segment triggered thousands of Amazon Echos to order, and pay for, doll houses without the consent of Amazon account holders.[7]
- In a recent court case, attorneys subpoenaed Amazon for the Amazon Echo data in the home where the murder allegedly occurred.[8]

What precautions can you take to limit your exposure?

1. If you're not using your device, Mute or Silence it. This keeps ambient noise such as commercials or conversations from accidentally activating the device.
2. Even though it may be convenient, you do not need to connect every account or service the device allows; if an account has sensitive information that you do not want shared, don't connect it to your personal assistant.
3. If the device holds recordings or maintains search histories, delete or clear them regularly.
4. Finally, and most importantly, share only what you want to share. Review and make the security settings on the device as tight as possible, using the manufacturer's provided tools and settings.

[4] https://www.cnet.com/news/weeping-angel-hack-samsung-smart-tv-cia-wikileaks/
[5] https://madeby.google.com/home/
[6] http://www.theverge.com/2017/2/5/14517314/google-home-super-bowl-ad-2017
[7] http://www.techtimes.com/articles/191846/20170109/alexa-caused-numerous-amazon-orders-for-dollhouses-across-san-diego-when-tv-report-mentioned-its-name.htm
[8] https://www.cnet.com/news/amazon-echo-alexa-agrees-to-hand-over-data-in-murder-case/

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Traveling Safely With Your Device

We don't know about you, but we can't even go to the store without our phone, much less to another country. But there are unique risks to traveling with your device: theft, hacking, malware, loss… Here are some tips to help you stay safe AND connected on your journey.

1 General Tips

- Decide if you truly need to bring the device with you.
  - » If you don't, just leave it home and ignore the rest of the list!
- No matter where you go, keep your eyes on your device.

2 Before You Leave

- Consider buying a cheap "burner" phone, and then get a SIM card when you arrive at your destination. Airports usually have them available.
- Make sure your phone's carrier plan includes your travel destination.
- If possible, avoid placing electronic devices in checked baggage; checked bags are often handled roughly.
- Remove all non-essential data from your device. Thieves may be as interested in the information they can sell as they are in the device itself.
- Use 2-factor authentication on all of your accounts.
- Lock your device with a password or PIN.
- Make sure that all of your software is installed and updated—operating system, firewall, antivirus, and all other security patches.
- Consider installing an app that allows you to wipe the data remotely, and one that tracks the device's location.
- Bring an electronic charger that will work in the new country and won't damage your device.
- Consider purchasing a privacy screen to protect the sensitive and private information on your screen from shoulder surfers.

3 International Laws

- Find out if your destination has any communication or censorship laws, or surveillance practices that are different from those in the US.
  - » Freedom House publishes a yearly Freedom on the Net publication that outlines the practices of many countries.
  - » You can find 2016's report at https://freedomhouse.org/report/freedom-net/freedom-net-2016.
- Follow all US Export Control Regulations.[1]

[1] http://research-compliance.umich.edu/export-controls

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

4 At the Airport/On the Plane

- At security screening, place your laptop in a bin by itself before you put it through the x-ray machine, and keep your eyes on it when it emerges.
- Keep your laptop under your seat; the overhead bin can put it at risk of falling.

5 At your Destination

- Be especially wary of online scams that may take advantage of your unfamiliarity with the location.

6 On a Cruise

- Cruises often cross into several international regions; make sure your phone's plan covers them all.
- The primary concern on a cruise is *cost* rather than *privacy*. Often your Internet and phone access are provided by the cruise line itself, and fees can be steep.
  - » This article has a good summary: http://www.cruisecritic.com/articles.cfm?ID=45
- Don't drop your phone over the side. (Just seeing if you were paying attention.)

7 At the Hotel

- If you have to leave your device behind for several hours, consider locking it in the safe rather than just leaving it in your room.
- Remember that most hotel networks are designed for ease of use, not security, so pay close attention to the points in the next tip.

8 Using Public Wi-Fi/Internet Cafés

Because we are more likely to use unsecured networks when we are traveling, here is a comprehensive list of safety tips for use on public Wi-Fi.

- Make sure you have permission before you connect to any network.
- Verify, with the owner, the name of any network before you connect to it; make sure it wasn't set up by a hacker.
- Avoid sending any confidential information over an open Wi-Fi network.
  - » This includes not only coffee shops, but airports, hotels, and city-wide networks.
  - » Usernames, passwords, bank account numbers, and sensitive work information can all be easily intercepted over an open wireless transmission.
- Use a VPN (virtual private network) if you must send confidential information.
- When you're finished, log out of any account you accessed and close all browsers.
- Don't check "connect automatically" on any public Wi-Fi network. Your phone may connect without your instructions, risking your privacy.
- For the same reason, turn off your Wi-Fi connection when you are not using it; it'll also save you some battery life.

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Design 101

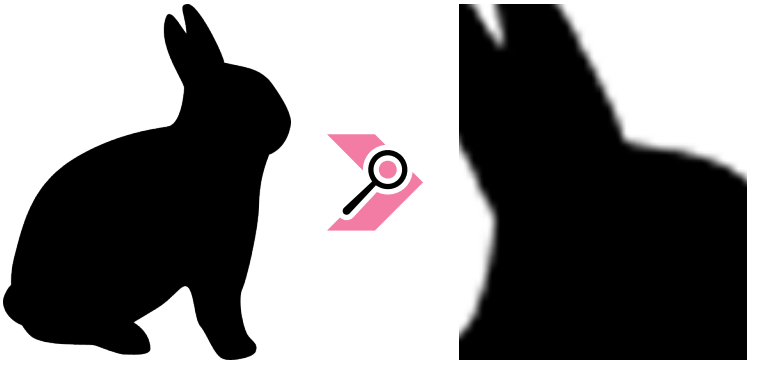
Working With Transparency

"Why is there white around the [insert object here] in my picture? It cuts into my other pictures!" Yes, it does, because whatever is in your picture is on a white background made of white pixels. Take this image of a hummingbird as an example. It looks like there's nothing but blank space around it.

In actuality, the area surrounding the hummingbird is made of white pixels. Since the standard for backgrounds, both on-screen and printed, is white, images with white backgrounds create the illusion of blank space. Unfortunately, the white pixels become displeasingly apparent when images are placed on areas of color.

So now you know that there are pixels there and, unfortunately, they aren't the easiest thing to get rid of. The reason for this deals with how the pixels build the image. In order for the pixels to simulate a realistic image, they are arranged in gradient patterns. If a black object sits on a white background, the pixels don't change from pure black to pure white. Instead, the black fades into the white with various shades of grey pixels in between, like in these pictures below:

This is what a black object on a white background looks like at 100% zoom, which is what it looks like when it prints. It might look like the black pixels change straight into white ones, but...



...if you zoom in close enough you'll see that there are various shades of grey pixels that lead the black into the white. This gradient stairstep creates the illusion of a smooth edge.

Florida Department of Law Enforcement (FDLE)
Florida Fusion Center (FFC)
Florida Infrastructure Protection Center (FIPC)

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

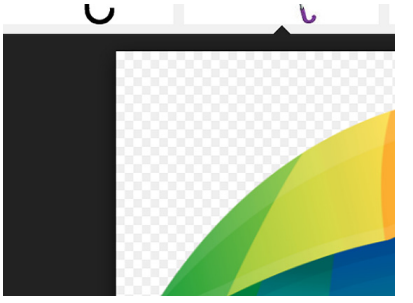
While this gradient effect makes objects look nice when they're on white backgrounds, trying to get rid of those pixels is easier said than done. Since the pixels that make an image are individually color-coded, going in and simply deleting the white pixels of the background isn't enough.

This is the result of getting rid of all pure-white pixels. The rim of pixels around the hummingbird are the remaining gradient pixels, all various shades of colors between the brown of the hummingbird and the white of the old background. In order to really get rid of a white background, each one of those pixels needs an opacity or color change to make them appropriatly transparent, and that can be easy or incredibly painstaking depending on the image.

Transparency is tied to file format. The format you want is PNG, the one that is supported on the web and supports transparency, as opposed to JPEG, which does not. PNGs show in your image searches, but they will likely be outnumbered by JPEGS. To make it easier, just add "PNG" to your image searches. The next question is, how do you recognize images with transparent backgrounds?

This is the pattern you'll be looking for.

When image searching, images might first appear to have white backgrounds but if you further select the image, you'll notice a grey checkerboard pattern. That pattern is a placeholder for the absence of pixels. Anywhere you see it, there are no pixels there. The example to the right shows the result of a Google search for "umbrella PNG." At first glance, it appeared that all the umbrellas were on white backgrounds, but selecting one by clicking on it reveals the grey checkerboard.



Pixel transparency also plays a role in cybersecurity. Bad actors have been known to embed malicious codes in individual pixels of website ads, obfuscating them by making slight changes to the original image's transparency (this is also known as malvertising).[1] Because it is so difficult to detect these changes with the human eye, we must rely on computers to detect the malware. Until ad companies get better at discovering these malicious ads, malvertising will continue to be a problem.

Overall, it's better to start with a PNG if you plan on placing images on non-white backgrounds and you don't want a white box with your image. If it becomes necessary to manually remove the white pixels, it is possible to do so, but it can be time-consuming depending on the image and could end up being more trouble than it's worth.

[1] https://arstechnica.com/security/2016/12/millions-exposed-to-malvertising-that-hid-attack-code-in-banner-pixels/

Dispatch Highlights

This section highlights articles from past *FIPC Dispatches* that our analysts think are noteworthy based on trends we're seeing in Florida. *The FIPC Dispatch* is a list of open-source articles that is sent out twice weekly. If you are interested in receiving *The FIPC Dispatch*, **let us know.**

To sign up for *The FIPC Dispatch*, visit SecureFlorida.org and click the **Sign up for The FIPC Dispatch** link at the bottom of the homepage and fill out the sign-up sheet or send an email to **FIPC@fdle.state.fl.us**.

This content is intended as an informative compilation of current/open-source cyber news for the law enforcement, cyber intelligence, and information security communities.

Know the risks of Amazon Alexa and Google Home

https://nakedsecurity.sophos.com/2017/01/27/data-privacy-day-know-the-risks-of-amazon-alexa-and-google-home/

- Voice-activated, web-connected devices like Amazon Alexa or Google Home are the latest and greatest in automated personal assistants. However, they come at a possible cost of compromising your privacy and security since they are always "listening," waiting for a voice command, and may retain much of what they "hear" on company servers.

  Analyst Note: Just like any other Internet-connected device, it is important to secure these devices. Be sure to properly patch and update them, and keep in mind what type of information they may be storing about you.

Over 1 million decrypted Gmail and Yahoo accounts allegedly up for sale on the Dark Web

http://www.ibtimes.co.uk/over-1-million-decrypted-gmail-yahoo-accounts-allegedly-sale-dark-web-1609882

- Stealing data for profit is an appealing enterprise for hackers, as evidenced by a dark web ad selling more than 1 million (purportedly stolen) decrypted email accounts and passwords.
- Most of these accounts appear to come from a variety of different reported breaches of third-party websites over the past decade.

  Analyst Note: These reports about dark web sales of stolen credentials underscore the importance of good password security. Always take care to create unique, complex passwords for every site you visit. If you think your account(s) can be illegitimately accessed by others, be sure to change your password(s) immediately.

How to scrub your private data from 'people finder' sites

http://www.infoworld.com/article/3168318/security/how-to-scrub-your-private-data-from-people-finder-sites.html

- There are a multitude of websites on the Internet that host personal details about you, your friends, and your family. The source of this information varies, but primarily comes from public record sites (such as your county's property appraiser).
- It is difficult to completely erase personal information about you on the Internet, but this article provides the methods for opting out from some of the bigger sites out there.

Analyst Note: Before we had the Internet, we had phone books, which gave out our names, addresses and phone numbers. Publication of personal information about you may be nothing new, but the Internet makes it easier for strangers to obtain. It's a good idea to "Google" your own name occasionally to see what data about you is on the web.

Personalized privacy app manages smartphone settings

http://www.csoonline.com/article/3164557/android/personalized-privacy-app-manages-smartphone-permission-settings.html

- Every mobile device app requires you to accept one or more settings when you download it. Some researchers are developing ways to track and manage these settings in one place, to make it easier for users to manage what they share.

Analyst Note: Although the application discussed in this article is still developing, it highlights an important topic. Always pay attention to what permissions an app requests when downloading it. Newer mobile operating systems allow you to disable certain features of an app.

Why criminals are using this old technique to take cyberattacks back to the future

http://www.zdnet.com/article/why-criminals-are-using-this-old-technique-to-take-cyberattacks-back-to-the-future/

- In recent years, spam and phishing emails have been on the decline. However, cybercriminals have begun using this tactic to spread malware again, particularly ransomware.
- As mobile device use continues to rise, malicious actors have many more opportunities to target unsuspecting users with malware.

Analyst Note: This is another cautionary tale about why it is important to always pay attention to a link before clicking on it, because all it takes is a tiny change to make something look authentic and trustworthy.

Contact us:
Phone: (850) 410-7645
Email: admin@secureflorida.org

Secure Florida's Best Practices for Office Security

1 Be suspicious of email links and attachments.

Emails designed to trick you into clicking links and downloading files come to inboxes daily. It is a practice called phishing and it's surprisingly effective. The easiest way for someone to get unauthorized access to your network is for you to give it to them. Never click on email links and never download attached files unless they are from trusted sources.

2 Use strong passwords and keep them private.

Your password is one part of the information security process that you control. Remember that you are protecting your accounts not only from someone trying to guess your password, but also from someone who steals password files to crack them. A strong password can take so much time to crack that it's not practical to keep trying, so the stronger your password is, the safer you are.

3 Back up your files regularly.

That spinning plate on your hard drive is an accident waiting to happen, and Florida is the lightening capital of the country. Hard drive crashes, electrical surges, and operator errors lead to many lost files. So do stolen laptops. Make sure you have backups of your important files.

4 Be careful when using public Wi-Fi.

When you connect to public Wi-Fi, or an "open network," anything you transmit can be seen by others. This includes usernames, passwords, account numbers, and confidential work information. Using a "secure" connection (such as HTTPS, SSL, or VPN) helps lessen the risk.

5 Use password protected screen savers.

It can only take a few minutes for someone to take advantage of a computer left idle.

6 Download only from approved sources.

As with email attachments, never download files from untrusted sources. Be especially suspicious of free software; it often has malicious software bundled with it.

7 Don't give out information to unverified individuals.

Social engineers try to fool you into giving out confidential information. Sometimes the information they ask for seems harmless, so their request doesn't raise any red flags. Before giving out any office-related information, be sure the person making the request is authorized to receive it.

8 Know and follow your organization's information security policies.

Your organization has its own security rules on matters such as using USB drives and personal devices on your work computer. Follow them carefully.

Information Resources

The Florida Infastructure Protection Center was established in 2002 to anticipate, prevent, react to, and recover from acts of terrorism, sabotage, cyber crime, and natural disasters. The FIPC is a team of cyber intelligence and critical infrastructure analysts who work to protect Florida's infrastructure.

SecureFlorida is an Internet safety and awareness outreach effort of the FIPC. Designed for the majority of computer users, Secure Florida covers all areas of computer, network, and communication security.

To sign up for alerts and other notices, **visit www.secureflorida.org/members/signup/**

The Beacon

The Beacon is published quarterly by Secure Florida to highlight cyber and critical infrastructure security information and awareness. **The Beacon** seeks to provide privacy and security information to all Internet users.

To read issues of **The Beacon**, visit **www.secureflorida.org/news/the_beacon/**

To sign up for **The Beacon**, visit **www.secureflorida.org/members/signup/**

The Dispatch

The FIPC Dispatch is compiled twice weekly by cyber intelligence analysts in the Florida Fusion Center. The content is intended as an informative compilation of current open-source cyber news for law enforcement, cyber intelligence, and information security communities.

To join **The Dispatch** mailing list, write to **FIPC@fdle.state.fl.us**

The **CSAFE** effort provides Internet safety presentations for organizations, clubs, schools, and businesses anywhere in Florida. For more information, visit **www.secureflorida.org/c_safe**

Class topics include:

- Best Practices for Internet Security
- Family Online Safety
- Combating Cyberbullying
- Online Safety for Seniors
- Identity Theft
- Mobile Communications
- Email Safety
- Internet Laws & Regulations