Atlanta Paralegal Association
May 17, 2018

Cybercrime

By: Parag Y. Shah

Shah Law Firm
1355 Peachtree St. NE
Suite 1800
Atlanta, Georgia 30309
(404) 844-4874
(404) 433-1136 (cell)
(404) 410-6933 (fax)
shah@shahlawfirm.com
www.shahlawfirm.com

Cybercrime is generally defined as any criminal offense that occurs through the use of the internet or computer technology. Probably the first thing that comes to people's minds is the act of hacking into a protected network online (known as a "cyberattack") for the purpose of mining information, planting a virus, sabotage, etc. However, cybercrime encompasses a lot of other online offenses as well – including identity theft, wire fraud (and other types of internet fraud), "phishing" scams (tricking people into giving personal information online), and more severe predatory practices such as child pornography. Many states have also begun passing laws against the practice of "cyber bullying," which is use of the internet to harass, persecute or threaten someone else.

- 50% of adults in the US have been victims
- $500 billion cost to the economy
- 20% of all businesses have been targeted
- 93% of all money is digital
- Most malware is on computers (or in business networks) for 3 to 4 **months** before it is detected (this is exactly what happened with Equifax)

There's a good chance words like "cybersecurity" and "hacking" are floating around the minds of Atlanta's internet users in light of the recent ransomware attack on the city's computer network or the data breaches that affected Equifax customers.

In 2014, 47 percent of adults in the U.S. had some of their personal information exposed by hackers, and a recent Gallup poll showed that 67 percent of Americans worry "frequently or occasionally" about cybercrime.

Falling victim to cybercrime is a scary thought, but there are steps people can take to protect themselves from malicious agents on the internet. WABE has compiled a guide to common internet crimes with tips on how Atlantans can avoid falling victim to them.

RANSOMWARE

Ransomware attacks affect victims large and small. It was a ransomware attack that left Atlantans without the ability to pay their bills for days in March, but these attacks can affect

individual users' computers as well. Once they're running on someone's machine, ransomware programs take control of the computer and threaten to restrict access to it indefinitely unless a ransom is paid.

Ransomware enters a computer or network either by "exploiting a security hole in vulnerable software or by tricking someone to install it," according to internet security company Norton.

Victims of ransomware might find themselves compelled to pay the money asked of them to get their data back, but the FBI states that's exactly what a user should not do. Ransomware should be removed by a "computer professional" because even when the malware appears to be gone, it could still be working in the background.

PHISHING SCAMS

Phishing is the act of luring in users with emails or phone calls that appear to be innocuous but are actually sent to trick users into giving away access to their computers, according to Microsoft. Phishing scams usually originate in spam emails or phone calls from people claiming to be with companies such as Microsoft saying they need to gain access to a user's machine.

It is relatively simple for attackers to disguise the emails they send to look like they originate from someplace official, be it a company's IT department or even Microsoft itself.

Clicking on a seemingly harmless link in an email can be a trigger to install malware or a route for hackers to access personal information. In 2017, phishing scammers managed to steal the paychecks of 27 Atlanta Public Schools employees, costing the district nearly $300,000, according to the AJC.

Microsoft recommends a few best practices for staying away from phishing scams: make sure to hover over links before clicking on them to be sure they go where they say they do. Be wary of official-looking emails that are full of spelling or grammar mistakes and be sure to double-check spelling on URLs that look official because a slightly misspelled web address could lead somewhere dangerous.

DATA BREACHES

All it took to put 56 million credit cards at risk and create $62 million in costs was a set of stolen log-on credentials for the computer network of Atlanta-based Home Depot, according to USA Today.

In addition to the credit card information that was stolen from self-checkout counters in Home Depot stores, millions of email addresses were stolen, leading to victims being at risk of further phishing scams.

One thing to remember is that, according to Experian, even though someone might be a victim of a data breach, they are not necessarily a victim of identity theft. The three steps the business services company recommends for people who have fallen victim to this are closely monitoring credit history and looking out for new accounts, keeping track of Social Security benefits and monitoring tax returns for unusual activity.

DENIAL OF SERVICE ATTACKS

A Denial of Service, or DoS attack, is when an attacker attempts to take down a computer or network by targeting it with a barrage of requests. Every attempt to access a website by typing a URL or clicking a link is a request, but large numbers of these at the same time can overload a server and prevent legitimate users from accessing a website or its content, according to the United States Computer Emergency Readiness Team.

In 2016, the University of Georgia's internet was brought to a halt by a Denial of Service attack that "saturated" the university's internet capacity of 20 gigabytes per second of data, blocking all access to the internet for everyone on campus, according to the AJC.

These attacks are difficult to prevent, simply because they take advantage of the way a server works. But many of these attacks utilize networks called botnet, which are computers connected by the same piece of malware that can all be used at the same time. While a user may not be able to prevent a DoS attack against a network, they could potentially avoid their computer

becoming the newest member of a botnet by remaining wary of phishing scams and ensuring their antivirus software is up to date.

CYBER SNOOPERS

Georgia, Virginia and Alaska — have no law against online "snooping," in which a hacker neither disrupts nor steals data. Georgia's governor has vetoed a bill that would have criminalized unauthorized computer access after receiving blowback from the state's booming cybersecurity industry.

The bill, vetoed by Republican Gov. Nathan Deal on Tuesday, would have made it a misdemeanor punishable by up to a year in jail to intentionally access a computer or network without authorization. The proposal passed the Georgia legislature in March amid the final chaotic hours of the legislative session.

The bill was designed to give law enforcement the ability to prosecute "online snoopers" — hackers who probe computer systems for vulnerabilities but don't disrupt or steal data. It follows the recent discovery by unauthorized independent cybersecurity experts of a vulnerability in the computer network where Georgia's elections are managed.

But a group of more than 50 academics, researchers, cybersecurity experts and technologists wrote Deal recently urging him to veto the bill, saying the legislation would chill security research and harm the state's cybersecurity industry.

PROTECTING YOURSELF

While anyone can be the victim of cybercrime, there are a few helpful tips to keep in mind. Norton recommends practices such as using long, difficult-to-guess passwords, keeping your network secured and using a full-service internet security suite.

SPECIFIC CRIMES

- Cyberattacks (often for the purpose of shutting down a computer system)
- Information theft (example: stealing trade secrets)
- Hacking (gaining illegal access to closed systems)
- Phishing (sending unsolicited emails to lure people into giving personal information)
- Theft of service (example: gaining Internet access without paying for it)
- Altering computer data unlawfully
- Solicitation (e.g., using the Internet to advertise the services of a prostitute, direct solicitation of sex for pay)
- Solicitation of a minor (using the Internet to lure a minor into an in-person meeting with the intention of sexual activity)
- Internet lewdness (subjecting a minor to verbal or graphic sexual content through the Internet)
- Possession and/or distribution of child pornography
- Fraudulent mass marketing / product misrepresentation
- eBay fraud
- Hacking and illegal access to computer systems
- Illegal downloading
- Identity theft

FEDERAL CYBERCRIME PENALTIES

Provisions of the Computer Fraud & Abuse Act

18 U.S.C. § 1030

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 yrs (20)
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 yrs (10)
Trespassing in a Government Computer	(a)(3)	1 yr (10)
Accessing a Computer to Defraud and Obtain Value	(a)(4)	5 yrs (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 yrs (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 yrs (20)
Negligently Causing Damage and Loss by Intentional Access	(a)(5)(C)	1 yr (10)
Trafficking in Passwords	(a)(6)	1 yr (10)
Extortion Involving Computers	(a)(7)	5 yrs (10)
Attempt and Conspiracy to Commit such an Offense	(b)	10Y for attempt but no penalty for conspiracy in section (c)

GEORGIA CYBERCRIME PENALTIES

Computer Theft - Uses a computer or network with knowledge that such use is without authority and with the intention of (1) taking or appropriating any property of another, whether or not with intent to deprive; (2) obtaining property by any deceitful means or artful practice; or (3) converting property in violation of an agreement. *OCGA 16-9-93(a)*.

Computer Trespass - Uses a computer or network with knowledge that such use is without authority and with the intention of (1) deleting or removing, either temporarily or permanently, any program or data; (2) obstructing, interrupting, or in any way interfering with the use of a program or data; or (3) altering, damaging, or causing the malfunction of a computer, network, or program, regardless of how long it persists. *Id. at (b)*.

Computer Invasion of Privacy - Uses a computer or network with the intention of examining employment, medical, salary, credit, or other financial or personal data relating to another with knowledge that such examination is without authority. *Id. at (c)*.

Computer Forgery - Creates, alters, or deletes any data contained in any computer or network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed "Forgery." Absence of a tangible writing directly created or altered by the offender shall not be a defense if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument. *Id. at (d)*.

Computer Password Disclosure - Discloses number, code, password, or other means of access to a computer or network knowing that such is without authority and results in damages to owner in excess of $500. *Id. at (e)*.

The three computer offenses of computer theft, computer trespass, and computer invasion of privacy include at least the following elements: (1) that the proscribed actions be taken with knowledge, (2) that the use of the computer or the examination of the other person's data was without authority, and (3) that the actions be taken with the requisite intent. *Sitton v. Print Direction, Inc.*, 312 Ga. App. 365 (2011).

"Without authority" includes the use of a computer or network in a manner that exceeds any right or permission granted by the owner of the computer or network. *OCGA 16-9-92(18)*; see *Wachovia Ins. Servs. v. Fallon*, 299 Ga. App. 440 (2009) (did not submit evidence establishing "knowledge that such use [was] without authority"). The jury may infer from the circumstances, including an employee's vindictive or retaliatory conduct, that the use of a computer was knowingly without authority. *DuCom*, 288 Ga. App. 555 (2007); see *Fugarino*, 243 Ga. App. 268 (2000).

For Computer Trespass, the burden on the State is not to show that defendant had completed the act of deleting or removing data from his computer but to show that he had used a computer, knowing that he did not have authority to do so, with the intention of deleting data. *Fugarino*.

Theft, Trespass, Invasion of Privacy, or Forgery, then up to 15Y and/or up to 50K fine. *OCGA 16-9-93(h)(1)*.

Password Disclosure, then up to 1Y and/or up to 5K fine. *Id. at (h)(2)*.

Civil relief available. *Id. at (g)*.

CYBERCRIMES AND THE FOURTH AMENDMENT

Riley v. California, Supreme Court of the United States, (2014)

Case Summary of Riley v. California:

- Riley was convicted of a shooting related offense after evidence seized from his cell phone (incident to his arrest) was used against him in court.
- Riley filed a motion to suppress which was denied and later appealed to the state's court of appeals claiming the search violated his Fourth Amendment rights.
- Riley, along with and similarly situated Wurie, petitioned the Supreme Court in a consolidated case.
- The Supreme Court held that the government may not conduct a warrantless search of a cell phone's contents that was seized after an arrest absent any exigent circumstances.

Statement of the Facts:

Officers pulled over Riley for a traffic violation, which led to his arrest on weapon-related charges. Riley was searched after his arrest and officers seized his cell phone from his pocket. Riley was convicted after a trial where evidence seized from his phone was introduced in a shooting related charge. In response, Riley appealed his conviction to the California state court of appeals. The court upheld the trial court's conviction.

Another defendant, Wurie, had his flip phone seized incident to arrest. Officers used the items seized in the phone to secure a search warrant to search Wurie's home. After the district court admitted the evidence found at the residence, Wurie appealed. The federal court of appeals found that the evidence was the fruit of an illegal search of the phone.

The cases were consolidated and the Supreme Court of the United States granted certiorari.

Procedural History:

The district court permitted the evidence to be introduced. On appeal the federal court of appeals reversed holding the evidence was the fruit of an illegal search of the arrestee's phone. The Supreme Court granted certiorari.

Issue and Holding:

May the government conduct a warrantless search of the contents of a cell phone seized after an arrest when no exigent circumstances exist? ***No.***

Rule of Law or Legal Principle Applied:

The government may not conduct a warrantless search of the contents of a cell phone that is seized incident to an arrest absent exigent circumstances, under the Fourth Amendment.

Judgment:

The judgment of the federal court of appeals is affirmed and the judgment of the state court of appeals is reversed.

Reasoning:

- **Generally, officers must obtain a warrant before conducting a search of the contents of a cell phone seized incident to an arrest. Otherwise, a Fourth Amendment violation occurs.**

The exception to search a person incident to an arrest is a valid exception to the warrant requirement of the Fourth Amendment. The exception is permitted for officer safety and to prevent destruction of evidence. However, no safety risk exists in a cell phone that warrants intrusion beyond a preliminary search to make sure the phone is not holding a weapon or small blade. The Court then distinguishes the warrantless search of a cell phone from other objects such as a cigarette container.

The Court then considers the separate indigent circumstances exception and whether it applies. The Court held that once officers have secured a cell phone, there is little risk of destruction of stored evidence. The concerns of protecting against remote wiping is beyond the concerns expressed in *Chimel v. California*, 395 U.S. 752 (1969), which is that an arrestee may destroy evidence that is within reach.

Although an individual's privacy rights are diminished once arrested, it should not be treated as a complete deprivation. The Court then distinguishes the search of a cigarette pack from the privacy invasion at issue regarding a search of a cell phone or residence and determines such a search is not constitutional. The search of the data on a cell phone is a major invasion of privacy due to the quality and quantity of information stored on phones.

The Court also concludes the government's assertion that under *Arizona v. Gant*, 556 U.S. 332 (2009), a warrantless search of a cell phone is justified when the cell phone is reasonably believed to contain evidence of the crime of arrest, applies to the search of vehicles and is inapplicable to a cell phone. Absent a warrant or demonstration of exigent circumstances, the government may not conduct a search of a cell phone incident to arrest.