

CYBERSECURITY FOR INDIVIDUALS AND SMALL BUSINESSES IN NEVADA

A RESOURCE FROM THE OFFICE OF THE NEVADA ATTORNEY GENERAL AND THE TECHNOLOGICAL CRIMES ADVISORY BOARD

PRESENTERS

- Information on the presenters

I. TRENDS IN TECHNOLOGICAL ID THEFT AGAINST INDIVIDUALS AND BUSINESS OWNERS

LEGITIMATE SOURCES OF PERSONAL INFORMATION

- Secretary of State
- County Assessor
- County Recorder
- City and County Business License Databases

PERSONAL INFORMATION THAT YOU PUBLISH VOLUNTARILY

- Personal social media accounts (e.g., Facebook)
- Professional social media accounts (e.g., LinkedIn)
- Blogs



SUMMARY OF PUBLICLY AVAILABLE PERSONAL INFORMATION

- Full name, and names of spouse and/or children
- DOBs
- Current and prior residential addresses
- Current and former employers
- Colleges attended, and when you graduated
- Companies and/or businesses that you own or manage, or used to, and their addresses
- Loans and other debts
- Phone numbers
- Email addresses

COMMON METHODS OF CYBER ID THEFT OF ADDITIONAL PERSONAL INFORMATION

- Phone, Mail, or e-mail Scams
- Ransomware and Malware
- Data breaches of Companies with Your PII
- Skimmers
- Good Ol' Fashioned Theft



HOW CRIMINALS USE YOUR INFORMATION

- Open New Accounts in Your Name
- Create Counterfeit Payment Cards Linked to Your Account
- File False Income Tax Returns
- Fraud May Occur Immediately, or in the Future.



TRENDS IN PHONE, MAIL, AND EMAIL SCAMS

- Utilities/IRS phone scam – A person calls you saying your utility will be shut off or that you owe taxes and you will be arrested unless you wire money. There are many variations of this (friend in jail/hospital/stuck overseas/immigration).
- Fake invoices, pay for government documents, directory scams
- Phishing – E-mail message that appears to be from a trustworthy source, but is actually someone trying to obtain your personal information

PROTECT YOURSELF: ALWAYS ASK QUESTIONS

PHONE SCAMS

- Individuals: Don't answer calls from unfamiliar numbers (realize that spoofing is a problem)
- Don't wire money to people you don't know
- Don't be afraid to hang up the phone
- Call an official number from an independent source
- You will always have warning of a power shut off, owed taxes, or pending arrest

DOCUMENT AND DIRECTORY SCAMS

- Many government documents and records are available for free to individuals and businesses. Check online or call and ask.
- Keep good accounting records and train employees on what services to send payments to.
- Sign up for electronic payments and bill pay to trustworthy sources.

PHISHING

- Don't click on links you receive via email; instead, visit the source or pick up the phone.
- Hover over email addresses and links to make sure they don't look fishy
- Businesses: Set a communication protocol, always follow it, and train your employees to do the same

RANSOMWARE AND MALWARE



- Ransomware – malicious software designed to block access to a computer system until a sum of money is paid.
- Malware – malicious software referring to any program harmful to a computer; in this case, stealing sensitive data.

PREVENTION IS THE KEY TO MALWARE

- Update your operating system and other software regularly on all devices (including smart phones)
- Look for secure connections (padlock in the browser and https)
- Use strong passwords (pneumatic devices and mixture of numbers, symbols and letters)
- Use multi-step verification, especially when you regularly sign on to accounts from elsewhere
- Train your employees in safe browsing practices; make strong passwords and multi-step verification a requirement
- Install anti-virus software
- Perform regular back-ups of your data, particularly for businesses



WHAT TO DO AS A RANSOMWARE VICTIM

1. CALL LAW ENFORCEMENT

Contact law enforcement and file a report. It is not likely they will be able to provide you with individual help, but every bit of information is helpful to stop thieves in the future.

2. TURN OFF AND DISCONNECT PC

If the computer is connected to any other device on the network (including smart phones and tablets), it could infect those as well. Take the computer offline and remove it from the network as soon as possible.

3. DON'T PAY THE RANSOM

If you have backed up your information, you will at least have access to that data. Realize that if you decide to pay the thief, it is still unlikely your data will be released back to you. The data may be gone forever.

4. Remove the Software: Check out www.nomoreransom.com, a site run by law enforcement and IT companies. You may also want to hire a professional.

II. WHAT SKIMMERS DO AND HOW TO SPOT THEM

SKIMMERS AND IDENTITY THEFT

- A skimmer is a device used to copy payment card numbers and personal identification numbers (PINs). Skimmers are installed at merchant locations, point-of-sale (POS) devices, automated teller machines (ATM), and stand-alone kiosks.
- Most of skimmers are very difficult to spot, even for law enforcement

PICTURES OF SKIMMERS – HENDERSON PD





TIPS FOR SPOTTING ATM SKIMMERS

- ATM skimmers are attached on or around ATMs for the purposes of capturing both the magnetic strip data and the PIN. They are made to be unobtrusive or to mimic legitimate components.
- Inspect the ATM for any signs of tampering. Lightly tug the area of the card slot; some are easily removed. Examine above the PIN pad for a small pinhole camera.
- Look for the following: a card slot that is loose or has fallen off; the presence of double-sided tape, glue, or pry marks around the card slot.
- Look for individuals who are tampering with the machine, who are intentionally covering their faces (with hats and sunglasses), who are spending a large amount of time around the machine without making a transaction, or someone showing up multiple periods of time.

TIPS FOR SPOTTING GAS PUMP SKIMMERS

- Gas pump skimmers can be installed externally over the card reader or internally. Commonly, it is an overlay over the card slot and/or PIN pad. Another device is placed inside the gas pump.
- Inspect the pump for any signs of tampering; business owners should also regularly check inside the pump for anything out of the ordinary.
- Lightly tug the area of the card slot. Like ATM devices, they are usually stuck to the outside with double-sided tape for quick removal.
- Look for similar signs as on the ATM devices: tampering, glue, out of the ordinary tape.

SKIMMERS: MINIMIZING YOUR RISK

- Cover the PIN pad while you enter your PIN. Keep your wits about you when you're at the ATM, and avoid dodgy-looking and standalone cash machines in low-lit areas, if possible. Stick to ATMs that are physically installed in a bank. Stand-alone ATMs are usually easier for thieves to hack into.
- Be especially vigilant when withdrawing cash on the weekends, as thieves tend to install skimming devices on a weekend — when they know the bank won't be open again for more than 24 hours.
- Keep a close eye on your bank statements, and dispute any unauthorized charges or withdrawals immediately.

III. DATA BREACHES: FOR INDIVIDUALS AND SMALL BUSINESSES

RECOVERING FROM DATA BREACHES AND GENERAL CYBER IDENTITY THEFT

DATA BREACHES

- A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so.
- Prevention is the key to surviving a data breach (both as an individual consumer and as the breached business)



- Different Breaches Target Different Categories of Information
- Payment Card Data Breaches (e.g. Target, Home Depot)
- User Account Data Breaches (Zappos)
- Medical Information Data Breaches (Anthem)
- Collectively, these breaches have the potential to expose financial account information, email addresses, usernames/passwords, drivers' license numbers, SSNs, healthcare ID numbers, and income data

MINIMIZING YOUR RISK: INDIVIDUALS

- Limit the amount of public information you voluntarily disclose
- Be suspicious of scare tactics
- Order and review your free annual credit reports at <https://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report>
- Fraud alerts and credit freezes
- Monitor your bank accounts regularly
- File tax returns as soon as possible

INDIVIDUALS: RECOVERING FROM A DATA BREACH OR ID THEFT



- Place a fraud alert on your account. To place a fraud alert, contact Experian, TransUnion and Equifax to let them know you are a victim of a data breach or ID theft and would like a fraud alert placed on your credit file. The alert is free and will stay on your credit report for 90 days.
- Order your credit report. You can order one free copy per year from each Credit Bureau at Annualcreditreport.com. Once you have a copy, dispute any errors you find with the credit reporting agency and fraud department of each business.
- Set up a credit freeze, if you are worried about damage to your credit. A credit freeze limits access to your credit and makes it more difficult for a hacker to open an account in your name. A credit freeze will last until you choose to remove it. Keep in mind that a credit freeze will require a fee of approximately \$10.
- Whether you place a fraud alert or a credit freeze on your account, you should still monitor your credit for potential fraud.

NEVADA LAW ON PERSONAL INFORMATION: DEFINITIONS

- Data collector: Any business entity that handles, collects, disseminates or otherwise deals with nonpublic personal information.
- Personal Information (PII): Includes a person's first name or first initial and last name in combination with any one or more of the following: social security number; driver's license, authorization card or ID card number; account number, credit or debit card number, in combination with the security code, access code or password permitting access to the person's financial account; medical or health insurance ID number; or a username or unique identifier in combination with a password, access code, or security question that would permit access to an online account.



NEVADA LAW ON PERSONAL INFORMATION: NRS 603A

- A data collector that maintains records containing the personal information of a NV resident must implement and maintain reasonable security measures to prevent unauthorized access, destruction, use, modification, or disclosure
- Additionally, any business that collects payment card information in connection with the sale of services must comply with the current version of the Payment Card Industry Data Security Standard. Ask your payment card servicer if it is PCI compliant, and familiarize yourself with the guidelines.

PCI IN A NUTSHELL




- The Payment Card Industry Data Security Standard is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
- The PCI DSS applies to any organization, regardless of size or number of transactions, that accepts, transmits, or stores any card holder data.
- The current PCI Data Security Standard can be found at the PCI Security Council's website at www.pcisecuritystandards.org.
- It is not enough that your third-party payment processor is PCI compliant (although that should be the standard to reduce risk exposure). Your business must also be PCI compliant.

SMALL BUSINESSES AND DATA BREACHES: THE BEST DEFENSE IS A GOOD OFFENSE

- Maintain and follow, without exception, a written data retention policy.
- Have a "crisis management plan" in place, and test it out
- Encryption is key; password and PIN protect EVERY device (don't forget smart phones). Change generic passwords on routers. Have all employees update their passwords regularly, and make sure the passwords are complicated. Use multi-step verification when possible.
- Make servers and files need-to-access: every employee does not need to get to every file
- Review system logs manually or use an automatic tool to check for suspicious activity
- Consider outsourcing your security.



STEPS TO TAKE AFTER A BREACH: SMALL BUSINESS



1. DON'T PANIC

This is when your crisis management plan should spring into effect. Seek an outside forensics team (preferably one you have previously vetted) and legal counsel as soon as possible to guide you through the next steps.

2. LIMIT DATA EXPOSURE AND DETERMINE SCOPE

Make sure you know how to isolate a system without simply turning it off. If the source computer is known, take it off the network. Determine what information was stolen and look for the source of the breach. Do not wipe the servers; this will destroy evidence that could help.





3. NOTIFY STAFF AND LAW ENFORCEMENT

Also alert your insurance company and any business partners. Regularly validate the contact information of these people ahead of time.

STEPS TO TAKE AFTER A BREACH

4. MANAGE THIRD-PARTY CONTRACTS

Ensure that all contracts with third-party service providers, hosting providers, and other relevant parties sufficiently address incident response management. These contracts should allow for your response team to review evidence from those environments.





5. ALERT AFFECTED CLIENTS

Nevada law requires that data collectors disclose a breach to affected victims "in the most expedient time possible and without unreasonable delay." NRS 403A.220(1). The timing should be decided with local law enforcement.



6. TREAT THIS AS A LEARNING EXPERIENCE

Find out where the weakness is, and improve next time.

ANY QUESTIONS?