



Nevada Attorney General's Tech Crimes Board

Cybersecurity Toolkit for NV Businesses

A guide to keeping your data and business safe



*Visit AG.NV.GOV for more information
or to download this toolkit*

CYBERSECURITY: Measures and practices designed to protect networks, computers and data against criminal or unauthorized attack or access.

Cybercriminals do not discriminate

Cybercriminals do not discriminate—they can target any and all types of vulnerable computer systems, including those belonging to large corporations, small businesses or individual, home users. In fact, a majority of Americans—64%—have personally experienced a major data breach.

With the rise in today's available technologies, employees are often connected to the Internet every day, conducting business, communicating with stakeholders and fellow employees, and sharing sensitive information. Businesses of all sizes are susceptible to attacks, especially small to medium-sized businesses that are often less prepared to manage security threats than their larger counterparts.

For today's businesses, falling victim to a cyber-attack is no longer a question of "if" but "when"

CYBERSECURITY TRAINING FOR EMPLOYEES

Cybersecurity is not only a threat limited to information technology and security professionals. The risks of cybersecurity extend to small businesses, organizations and boardrooms. Employee training is instrumental to a successful cybersecurity protection program, and an effective way of ensuring all staff understand cyber threats and how to avoid falling victim to them.

In 2016, it was estimated that about **80%** of all U.S. companies have fallen victim to a cyber-attack.

A recurring cause of cyber-attacks is social engineering, or specific tactics cybercriminals use to manipulate individuals in order to access private data or corporate systems. The easiest means of obtaining information and access is to find ways to get a user to give you his/her passwords and sensitive information. Cybercriminals know this and continue to find more and more ways to obtain this type of information from users.

Help your employees help themselves



5 TYPES OF SOCIAL ENGINEERING SCAMS:

Phishing: Phishing attacks use email, websites, website ads or chats to infect your machine with malware and viruses to collect personal and financial information. The provided links are designed to look like the real thing—often impersonating a real financial institution, government agency, business, service or individual. When users respond or click on the links, cybercriminals take the opportunity to access their personal information and accounts.






Baiting: Similar to phishing, baiting involves enticing a user by offering something in exchange for private data. The “bait” can be in the form of coupon rewards, movie or music downloads, or even a flash drive left out on a desk for a user to find. If a user bites at the bait, malicious software is directly delivered into the victim’s device.

Quid Pro Quo: Similar to baiting, quid pro quo involves a specified service in exchange for private data. In this case, the “bait” is a provided service, such as a hacker posed as a technology expert offering to help solve a user’s IT problems and convincing the user that providing his/her login credentials are necessary in order to resolve the problem.

Pretexting: When a cybercriminal impersonates a boss or co-worker to create a false sense of trust between the user and themselves in order to gain access to private data. A hacker could pose as a member of an office’s IT team asking the user for private data in order to complete a survey or audit.

Tailgating: Tailgating involves an unauthorized person who gains access to private or sensitive data by physically following or “tailgating” an employee into a restricted area. This attack can take many forms—including when a hacker asks an employee to borrow a private laptop or phone for a few minutes, or when a hacker calls out to an employee asking him/her to keep the door or elevator open because he/she has forgotten their key card.

SIMPLE TIPS TO BE CYBER SECURE AT WORK

-  **Guard your devices:** In order to prevent unauthorized access and potential theft, never leave your laptop or mobile device unattended in a public place. Always lock your devices when they are not being used.
-  **Secure your accounts:** Use passwords that are at least eight characters long and a mix of letters, numbers, and characters. Using a passphrase such as a news headline or even a title of a book is often helpful. Avoid sharing any of your usernames or passwords with anyone, including coworkers.
-  **Back it up:** Make electronic and physical back-ups or copies of all your important work. Data can be lost in many ways including computer malfunctions, malware, theft, viruses, and accidental deletion.
-  **Stop and think:** Before opening attachments or clicking links in emails, exercise caution. Links in email, online chats, and online posts are often the way cybercriminals compromise your devices.
-  **Report anything suspicious:** If you experience any unusual problems with your computer or device, report it to your IT Department or an authoritative figure.

SPOTTING CYBER SCAMS



From: "AT&T via DocuSign" <dse@docuSign.net>
Subject: Please DocuSign this document: Contract_changes_08_27_2014.pdf
Date: August 27, 2014 at 8:37:31 AM MST
To: <atyourservice@komando.com>

Please review and sign your document Company Logo

From: AT&T (service@att.com)

Hello,

AT&T Contract Changes has sent you a new DocuSign document to view and sign. Please click on the 'View Documents' link below to begin signing.

[View Documents](#)

Alternately, you can access these documents by visiting docuSign.com, clicking the 'Access Document' link, and using this security code:

700L63FZ45AD4870BB791C1EN0L8L20W1

This message was sent to you by AT&T who is using the DocuSign Electronic Signature Service. If you would rather not receive email from this sender you may contact the sender with your request.

If you need assistance, please contact DocuSign Support (service@docuSign.com)

TIP: Ensure all employees are wary of emails that require them to click on links or that contain attachments they aren't expecting. Before clicking on anything, take measures to confirm with the sender or review your personal account information.



Dear valued Verizon customer,

It has come to our attention that your Verizon information needs to be reactivated as part of our continuing commitment to protect your account and to reduce fraud. Once you have reactivated your Verizon records, your account service will not be interrupted and will continue as normal.

To reactivate your Verizon account click on the following link:

[Click here to verify your Verizon account](#)

Thank you.

Failure to verify your records will result in a account suspension.

Verizon will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and Terms of Service if you have any questions.
<http://www.verizon.com>

Copyright © 2015 Verizon

THE FBI FEDERAL BUREAU OF INVESTIGATION

ATTENTION! YOUR COMPUTER HAS BEEN LOCKED
Please read carefully the information below in order to avoid further deterioration of the situation.

By the 18 USC § 2256 you have broken the U.S. laws that prohibiting the possession and distribution of survey using materials containing child porn, bestiality and/or distribution of video \ photo materials and pirated software. According to Pub. L. 112-123 Penalties range from fines to imprisonment. Please stop further action in order to avoid much more strict punishment. You will be responsible to the Supreme Court of the United States for the next steps.

Under the paragraph 1466A viewing of the above-listed materials also punishable and you break the law of - Obscene visual representations of the sexual abuse of children. We inform you that all internet traffic is monitored by state agencies, law enforcement services will be notified about this event.

One time violations of the law provides exempts \ blocking of the Computer with the ability to pay an administrative fine of \$200, subsequent violations can be punished up to imprisonment.

VIDEO AND AUDIO RECORDING

Your IP address: 66.85.134.158

ILLEGAL CONTENT DETECTED ON YOUR PC

ENTER MONEYPAK CODE HERE (\$200)

Why do we use the MoneyPak?
if you do not want to pay a fine.

WHERE CAN I BUY THE MONEYPAK?

Walmart CVS K Mart 7-Eleven Walgreens

abuse@fbi.gov
FBI.gov is an official site of the U.S. government, U.S. Department of Justice

McAfee
An Intel Company



RED FLAG: Missing sender or recipient information, generic greetings, misspelled email addresses, and email addresses that don't exactly match the company name. Any emails that ask the recipient to download a form or click to verify or complete a task are highly suspicious and an employee should NOT click on anything. Instead, report the email to IT immediately.

CYBERSECURITY CHECKLIST

Businesses face significant financial loss when a cyber-attack occurs. **Cybercriminals rely on human error**—such as failing to install or update software patches, clicking on phishing links, or falling for a number of cyber baits and scams—**to gain access to systems and private data**. Cybersecurity requires vigilance from the executive team down to a newly hired employee.



- ✓ Conduct a security risk assessment to understand potential security threats and the impact they may have on your business. Use this information to shape a security strategy that meets your specific needs.
- ✓ Train your employees. An ongoing and mandatory annual or semi-annual training plan should be implemented for all employees, even if the training is provided online to address the evolutions in cybersecurity threats. The training should include examples of threats, as well as instruction on security best practices.
- ✓ Create straightforward cybersecurity policies. Write and distribute a clear set of rules and instructions on cybersecurity practices for employees. This will vary from business to business but may include policies on using personal devices, accessing social media, etc.
- ✓ Control access to computers. Use key cards or similar security measures to control access to facilities, and ensure that employees use strong passwords for laptops and desktops. Administrative privileges should only be given to trusted IT staff.
- ✓ Protect your network and devices. Implement a password policy that requires strong passwords that expire every 90 days. Deploy firewall, VPN and antivirus technologies to ensure your network and endpoints are not vulnerable to attacks. Consider implementing multifactor authentication. Ongoing network monitoring should also be considered essential.
- ✓ Keep software up-to-date. It is essential to use up-to-date software products and to be vigilant about patch management. Cyber criminals exploit software vulnerabilities using a variety of tactics to gain access to computers and data.
- ✓ Back up your data. Daily backups are a requirement to recover from data corruption or security breach losses. Consider using a modern data protection tool that takes incremental backups of data periodically throughout the day to prevent data loss.
- ✓ Know where your data resides. Maintaining oversight of business data is an important piece of the security puzzle. The more places data exists, the more likely it is that unauthorized individuals will be able to access it.

REPORTING A CYBERCRIME

By reporting cybercrime to the appropriate authorities, each one of us can play a role in making the Internet safer and more secure for everyone. If you have fallen victim to a cybercrime, immediately notify your local authorities to file a complaint. Keep records of all evidence related to the incident and the suspected cybercriminal. Below is a list of government agencies and organizations that review cybercriminal complaints.

US-CERT.gov

Report computer or network vulnerabilities to US-CERT via the hotline (1-888-282-0870) or the website (www.us-cert.gov). To report phishing attempts to US-CERT, forward phishing emails or websites to US-CERT at phishing-report@us-cert.gov.

IC3.gov

If you are a victim of online crime, file a complaint with the Internet Crime Compliant Center (IC3) at www.ic3.gov. IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

FTC.gov

Report fraud to the Federal Trade Commission at www.ftc.gov/complaint , if applicable. Report identity theft at www.IdentityTheft.gov, the government's free, one-stop resource to help you report and recover from identity theft.

SSA.gov

If you believe someone is using your Social Security number, contact the Social Security Administration's (SSA) fraud hotline at 1-800-269-0271. For additional resources, visit the SSA at <http://oig.ssa.gov/report-fraud-waste-or-abuse>.

