Snell & Wilmer
Committed to being your perfect fit.™

Denver Emerging Business Seminar: Data Privacy and Cybersecurity Considerations

March 17, 2021

Aloke Chakravarty

swlaw.com

The Emerging Business Seminar Series

- Focused on entrepreneurs and emerging growth companies
- Hands-on, how-to programs offering timely and practical tips
- Designed to help take the entrepreneur from company formation to liquidity
- Held **monthly on the third Wednesday** – stay tuned for information on upcoming seminars

About the Presenter

- Aloke Chakravarty, Partner
- Co-chair of Snell & Wilmer's Investigations, Government Enforcement and White Collar Protection
- Focuses on cybersecurity, data protection and privacy
- Twenty years of experience as a state, federal and international investigator, prosecutor and trial lawyer

Aloke Chakravarty
Partner, Snell & Wilmer
achakravarty@swlaw.com
303.634.2121

SMALL BUSINESSES ARE ON FRONT LINES OF GLOBAL CYBERWAR

90%
OF SMALL BUSINESSES DON'T USE ANY DATA PROTECTION

SOME ESTIMATES INDICATE THAT **58 PERCENT** OF CYBER ATTACKS ARE TARGETED AGAINST SMALL BUSINESSES

THE FINANCIAL LOSES CAN BE DEVASTATING

54%
OF ALL CYBER ATTACKS RESULT IN MAJOR FINANCIAL DAMAGES RESULTING IN MORE THAN[4]
$500,000

$34,604
IS THE AVERAGE COST OF A BREACH FOR A SMALL BUSINESS[5]

ATTACKS INCLUDE:

PHISHING
MALWARE
RANSOMWARE
AND MORE

40%
OF RESPONDENTS EXPERIENCED **8 OR MORE HOURS** OF SYSTEM DOWNTIME DUE TO A SECURITY BREACH

39%
OF THOSE RESPONDENTS REPORTED THAT AT LEAST **HALF OF THEIR SYSTEMS** HAD BEEN AFFECTED BY A SEVERE BREACH[6]

44%
OF SMALL BUSINESSES HAD AT LEAST 2 TO 4 CYBER ATTACKS IN THE PAST YEAR[7]

[4] https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf; [5] https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf; [6] https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf;
[7] https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

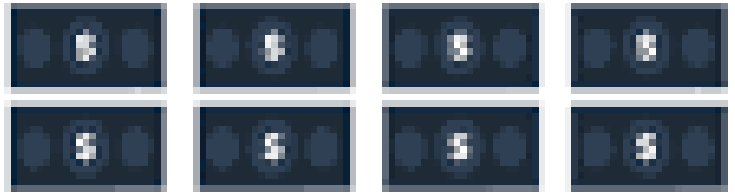
SMALL BUSINESSES ARE VULNERABLE TOO

72% OF CYBER ATTACKS AFFECT COMPANIES WITH **LESS THAN** **100** **EMPLOYEES**

SMALL ≠ SAFE

OF SMALL BUSINESSES THINK THEY ARE TOO SMALL TO BE HACKED

THE COST IS HEAVY



$188,242

THE AVERAGE AMOUNT IT TAKES A SMALL BUSINESS TO RECOVER FROM A CYBER ATTACK

Courtesy Quadratics

National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

If you forget your password (or you think somebody else knows it), tell your IT department as soon as you can.

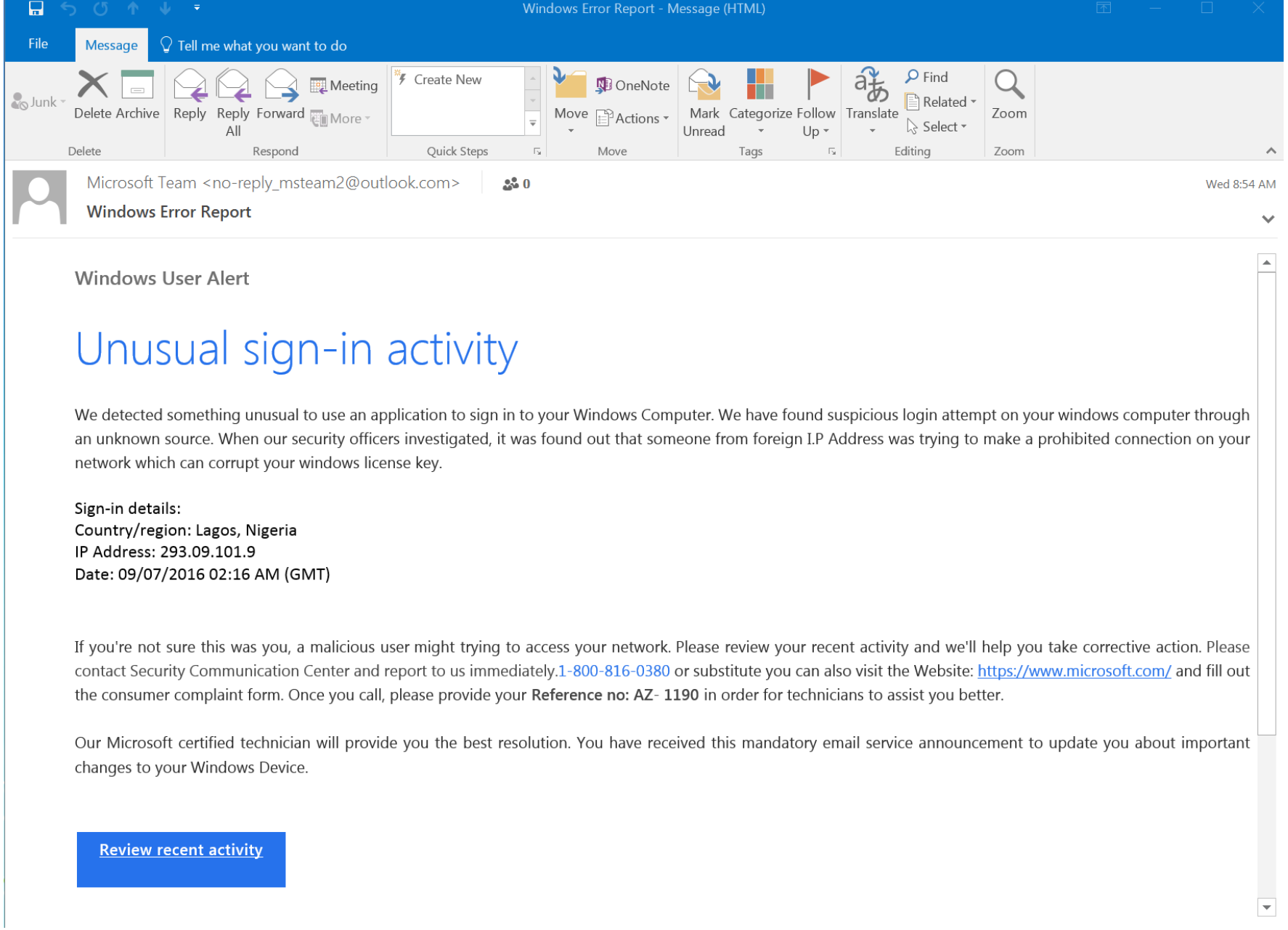
Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

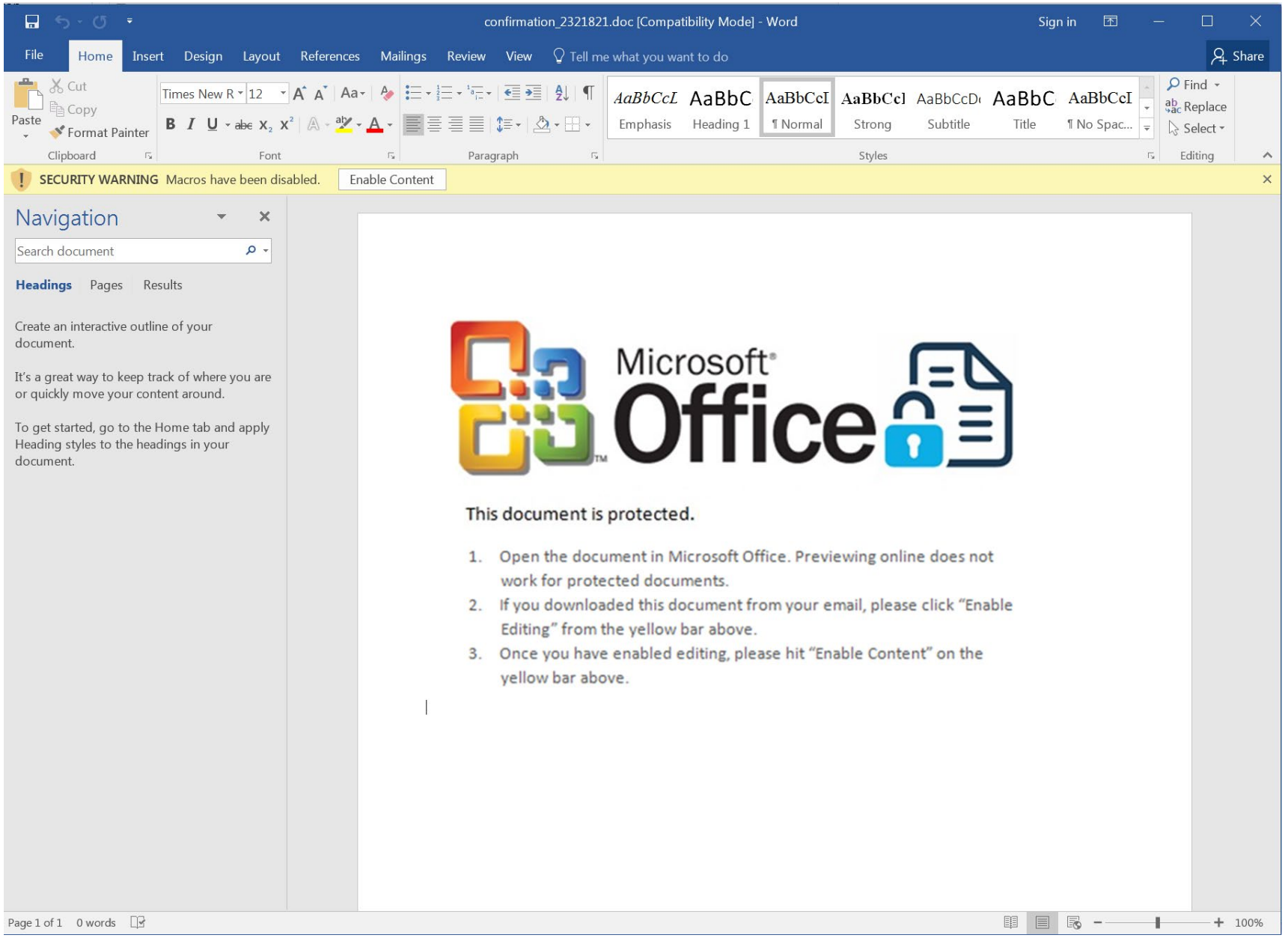
Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

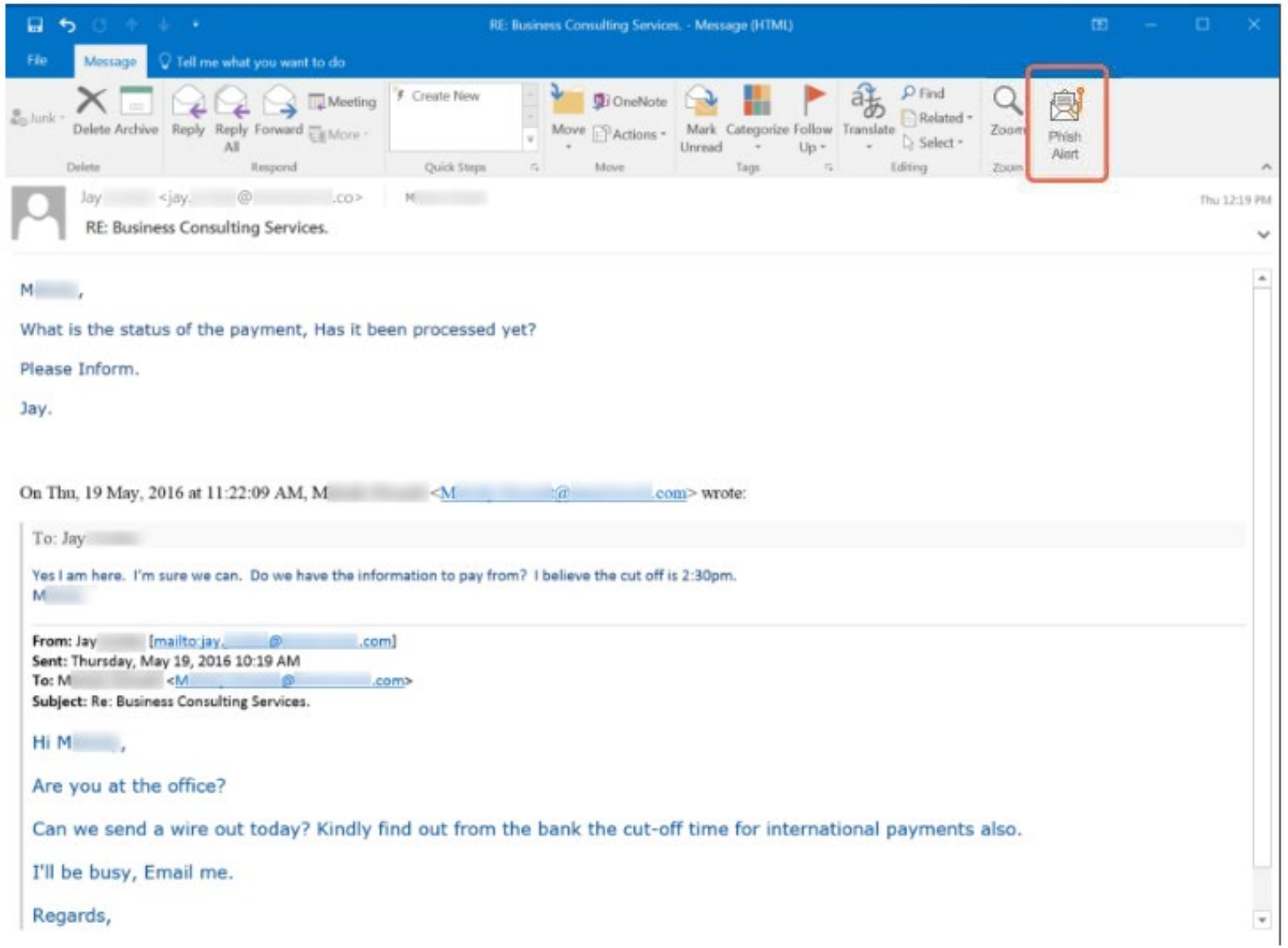
Consider using a password manager, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.

Sample Threat Vectors

- Phishing (examples courtesy Phishing.org)
  - Credential harvesting
  - Business email compromise
  - Ransomware package deployment




confirmation_2321821.doc [Compatibility Mode] - Word
Sign in
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do
Share
Paste
Cut
Copy
Format Painter
Clipboard
Times New R
12
Font
Paragraph
Emphasis
Heading 1
¶ Normal
Strong
Subtitle
Title
¶ No Spac...
Styles
Find
Replace
Select
Editing
SECURITY WARNING Macros have been disabled.
Enable Content
Navigation
Search document
Headings
Pages
Results
Create an interactive outline of your document.
It's a great way to keep track of where you are or quickly move your content around.
To get started, go to the Home tab and apply Heading styles to the headings in your document.
Microsoft Office
This document is protected.
1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.
Page 1 of 1
0 words
100%


RE: Business Consulting Services. - Message (HTML)
File
Message
Tell me what you want to do
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Delete
Respond
Create New
Quick Steps
Move
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
Zoom
Phish Alert
Jay <jay. @ .co>
M
Thu 12:19 PM
RE: Business Consulting Services.
M ,
What is the status of the payment, Has it been processed yet?
Please Inform.
Jay.
On Thu, 19 May, 2016 at 11:22:09 AM, M <M @ .com> wrote:
To: Jay
Yes I am here. I'm sure we can. Do we have the information to pay from? I believe the cut off is 2:30pm.
M
From: Jay [mailto:jay. @ .com]
Sent: Thursday, May 19, 2016 10:19 AM
To: M <M @ .com>
Subject: Re: Business Consulting Services.
Hi M ,
Are you at the office?
Can we send a wire out today? Kindly find out from the bank the cut-off time for international payments also.
I'll be busy, Email me.
Regards,

COVID-19 – Increase in Cyberattacks

- Pandemic has served as catalyst for hacking increases in 2020
  - Weekly COVID-19 related phishing attacks grew from 5,000 in February to more than 200,000 in late April
  - World Health Organization experienced a 500 percent increase in attacks
  - Since January, over 4,300 domains related to coronavirus-related stimulus or relief packages have been registered globally
  - FBI's Internet Crime Complaint Center reported a 400 percent increase in online crimes reported since pandemic began
- Other notable trends
  - Mobile exploits diversify
  - Cloud exposure

Source: SC Media, FBI

California Consumer Privacy Act (CCPA) Main Features

- Knowledge: must be able to learn what personal information is being collected, how it is being collected and used, and whether and to whom it is being disclosed or sold
- Sale of Data: must be easy to opt out of having personal information "sold" (broad definition) to a third party and must be opt-in for under 16 consumers *before* sale
- Data Removal: may request deletion of personal information and must be informed of this right
  - Exception if data needed to complete a transaction
- Service Equality: cannot discriminate against consumers who exercise their privacy rights
- Private and Public: causes of action and fines

California Privacy Rights Act of 2020 (CPRA)

- Passed in November 2020 (by initiative) and set to go into effect January 1, 2023
- Amends the California Consumer Privacy Act of 2018 (CCPA)
- Expands the CCPA's scope and introduces additional privacy protections for California consumers
- Exception for employees and business-to-business extended until January 1, 2023

CPRA Amendments to CCPA

- Includes new definitions (i.e. contractors), categories of sharing (cross-context behavioral advertising within organization and externally), Sensitive Personal Info
- Includes expanded individual rights, including access to information, correcting information and opting out of certain data-sharing arrangements
- Has records minimization requirements – keep only as long as necessary
- Requires agreements to be in place for data sharing
- Regulations likely by 2022; New enforcement agency and expanded private basis for lawsuits
- Consider the following: Data Categorization
  - Strengthen records retention policies
  - Develop strategy for third-party independent contractors
  - Update contracts, websites and privacy policies

New Terms

Cross-context behavioral advertising:
"[T]he targeting of advertising to a consumer based on the consumer's **personal information obtained from the consumer's activity** across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."

New Terms

Sensitive Personal Information (“SPI”)

- Lists various categories of information, including (but not limited to):
- SSN, state ID, DL number, passport number
- financial account or debit/credit card information + a code/password that would allow access to an account
- racial or ethnic origin
- contents of consumer’s mail, email, or text messages
- genetic data

New & Expanded Rights

Right to Correct Inaccurate Information

- Consumer may request a business correct inaccurate personal information it maintains about the consumer
- Business must disclose the consumer's right to request correction of inaccurate PI
- Upon receipt of a verifiable consumer request to correct inaccurate PI, business must use "commercially reasonable efforts" to correct it, as directed by consumer

New & Expanded Rights

Right to Know What PI Is Shared, and With Whom It Is Shared

- Consumer may request the business disclose to the consumer the categories of PI collected and shared, and the categories of third parties with whom it was shared

  Note: this addition supplements the pre-existing right to know regarding a businesses' sale of information already in the CCPA

- Increases look-back period for right-to-know past 12 months
  - Unless doing so is "impossible or would involve a disproportionate effort"
  - Only applicable to PI collected on/after Jan. 1, 2022

New & Expanded Rights

Right to Opt-Out of Sharing PI

- Consumer may, at any time, direct the business not to share the consumer's PI
- Business must provide notice to consumers that information may be shared, and that consumer has right to opt-out of the sharing

    Note: this supplements the pre-existing right to opt-out of the sale of information already in the CCPA

New & Expanded Rights

Right to Delete

- Business must notify **contractors and third parties** to delete the consumer's information, unless "impossible or involves disproportionate effort"
  - Before, only had to notify service providers
- Need not comply with request if not **"reasonably"** necessary for the business to accomplish certain tasks, including to:
  - Help ensure "**security and integrity**"
  - Fulfill the terms of a written warranty or product recall in accord with federal law

New Limitations & Obligations for Businesses

- May only retain collected PI as long as "**reasonably necessary**" to achieve its disclosed purpose
- May only use, retain, and share PI as "**reasonably necessary and proportionate**" to achieve the purpose for which it was collected
  - May not further process PI in a way incompatible with disclosed purposes

New Limitations & Obligations for Businesses

Must implement **reasonable security procedures & practices** "appropriate to the nature of" PI collected, to protect from:

- Unauthorized/illegal access
- Destruction
- Use
- Modification
- Disclosure

New Relationship Structures

"A business that collects a consumer's PI and that …**shares** it with, a third party or that discloses it to a service provider or contractor for a business purpose **shall enter into an agreement** with such third party, service provider, or contractor," that meets certain requirements.

Private Right of Action—Expanded

- Now also applies to unauthorized access and exfiltration, theft, or disclosure of an **email address + password/security questions** that would allow access to account
- 30-days' written notice and cure period still applies, but clarifies that "[t]he implementation and maintenance of reasonable security procedures . . . ***following*** a breach" does not cure.

Colorado Data Privacy Requirements

- There are three primary components to Colorado's data security laws (C.R.S. § 6-1-713 et seq.).
- Colorado requires certain persons and entities that maintain personal identifying information (PII) in paper or electronic form to establish written policies governing the disposal of PII.
- Colorado law requires certain persons and entities to take reasonable steps to protect PII.
- The law requires notification of security breaches affecting personal information (PI), which includes detailed notice to Colorado residents and, in certain circumstances, notice to the Attorney General.

Colorado Proposed Data Privacy Legislation

- Modeled on California privacy framework
- Opt out of certain information sharing
- Data subject access/deletion rights
- Risk assessment requirement
- Jurisdictional thresholds
- Enforcement mechanism

Data Privacy Best Practices

- Data mapping
- Vendor management
- Transparency
- Cybersecurity testing/auditing
- Clear internal governance structure
- Culture of cybersecurity and data privacy

Data Breach Response

A covered entity that maintains, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware that a security breach may have occurred, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused.

C.R.S. § 6-1-713 (2)(a)

Data Breach Considerations

- Breach notification requirements
- Third party liability
- Regulatory liability
- First party liability
- Class action exposure
- Insurance
- Vendor management
- Law enforcement notification
- Reactive steps toward threat actors

Establishing the Attorney-Client Privilege

- After a cyber incident occurs, traditionally first reach out is to outside counsel
- Outside counsel will retain, on behalf of company, necessary vendors to investigate cyber incident
  - Forensic investigator
  - Breach notification provider
  - Credit monitoring provider
- Because outside counsel hires the vendors, and not the company, vendor work product is typically protected under attorney-client privilege

Duty to Notify

- Notice to Colorado residents must include the following:
- The date, estimated date, or estimated date range of the security breach;
- A description of the personal information that was acquired as part of the security breach (or that is reasonably believed to have been acquired);
- Information that a resident can use to contact you to inquire about the security breach;
- A statement that the resident can obtain information from the Federal Trade Commission (FTC) and the credit reporting agencies about fraud alerts and security freezes;
- The toll-free numbers, addresses, and websites for consumer reporting agencies;
- The toll-free number, address, and website for the FTC.

Colorado Attorney General Notification

If notice is required to the Attorney General, provide the following in your notice to the Attorney General:

- The name of your organization and a primary contact who can be reached for further information;
- The date you learned there may have been a security breach;
- The date you determined that a security breach occurred;
- The date that you provided notice to impacted Colorado residents;
- The number of Colorado residents impacted by the breach;
- Total number of individuals impacted by the breach; and
- A copy of the notice you provided to Colorado residents.

Priority Compliance Milestones to Consider

- Update the privacy policy on the website
- Establish a method for providing notice at collection of PI
- Provide a way for consumers to submit requests
- Develop a process for verifying and responding to consumer requests
- Train relevant personnel
- Implement reasonable security procedures and practices
- Review third-party contracts. Implement data protection language that prohibits vendors from selling that PI, require them to delete PI at the firm's request, obligate them to implement reasonable security measures to protect the PI, and otherwise cooperate with the firm's data privacy compliance.
- Firms that are considered service providers or third parties should review their obligations and prepare a compliance plan
- Employee notice

Protective Measures to Consider

- Create culture of compliance
- Risk-based prioritization and assessment
- Investment of resources – data mapping and cybersecurity
- Implement Compliance Program
  - Policies – internal facing – Infosec, DSARs
  - Authority and Responsibility – gravitas and influence
  - Training – anyone involved in handling PI
  - Communication – constructive feedback
  - Monitoring and Response – act on it

Thank You

Aloke S. Chakravarty, Partner,
Cybersecurity, Data Protection and Privacy

Co-Chair, White Collar Defense & Investigations
303.634.2121 | achakravarty@swlaw.com

www.swlaw.com/blog/data-security

Denver Emerging Business Seminar Series

- April 21, 2021 at 10 am MDT
- Key Corporate and Tax Issues Every Startup Should Consider at Formation

Bill Kastin

Partner, Snell & Wilmer

Tax Practice Group