



Cybersecurity Best Practices for Benefit/HR Policies

Vaughn Manning, CISSP

DFW ISCEBS
Thursday, February 8

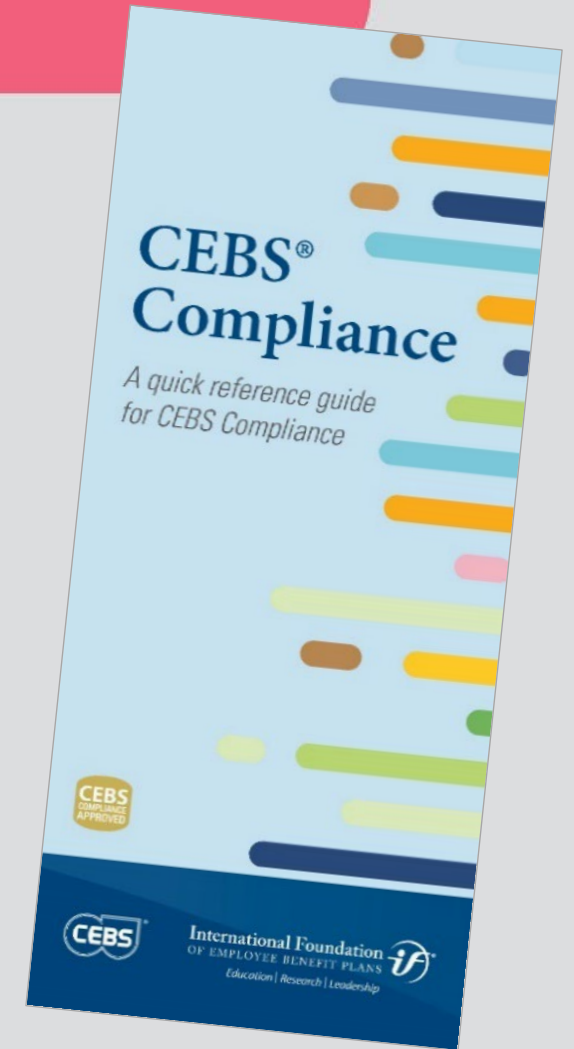


Self-Report Your Credit

- This program qualifies for CEBS Compliance credit
- Be recognized for the professional education you complete to stay up-to-date
- 30 credits over two calendar years to be compliant
- Credits are self-reported



Scan to
self-report CEBS
compliance credit
from today's
session!



ISCEBS Membership

- Join or renew today!
- CEBS students and graduates can join
- Add membership to your local chapter!
- Join online at www.iscebs.org/join

Member Benefits

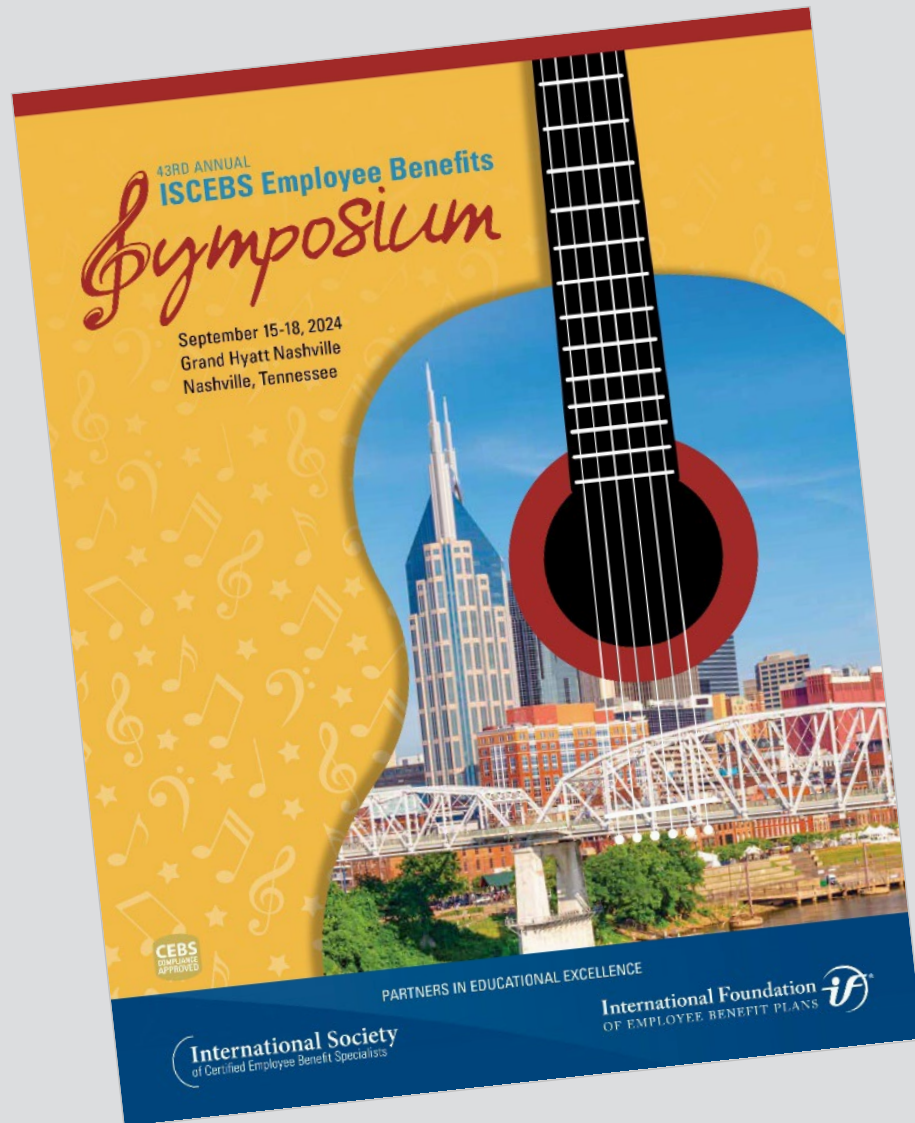
- Local chapters
- Unlimited webcasts
- Discussion forums
- Personalized research
- Membership directory
- *Benefits Quarterly* and *NewsBriefs*

ISCEBS Gold Member

- Society members have the opportunity to attain ISCEBS Gold Membership—An exclusive level of recognition representing both your CEBS Compliant status and your affiliation with ISCEBS.



43rd Annual Symposium



- September 15-18, 2024
- Grand Hyatt Nashville
- Nashville, Tennessee

CEBS Designation— Take Your Education to the Next Level



CEBS

Certified Employee Benefit Specialist® Program

www.cebs.org

CEBS® ACADEMIC PARTNER



DALHOUSIE
UNIVERSITY

Refer a Friend to CEBS!

- Let a colleague know about the CEBS program and the opportunities it presents! CEBS also offers a new Success Package for each course that is a 20% discount when you purchase the study guide, textbook, online study group and exam.



Are You Using Your Digital Badges?



Learn how to access and use your badges at
www.ifebp.org/digitalbadges

The phish I sent at the height of COVID uncertainty, and the Benefit Director's response...

From: Aetna <noreply@billing-aetna.com>
To: [Redacted]
Subject: COVID-19 Insurance Coverage: Thank you for your purchase!
Send Date (UTC): 4/10/2020 3:09:58 PM
[Download Original Item](#)



Insurance coverage update alert

Thank you for purchasing Coronavirus (COVID-19) insurance coverage from Aetna.

Please remember to find your latest billing statement in the link provided below:

[Here's your Bill](#)

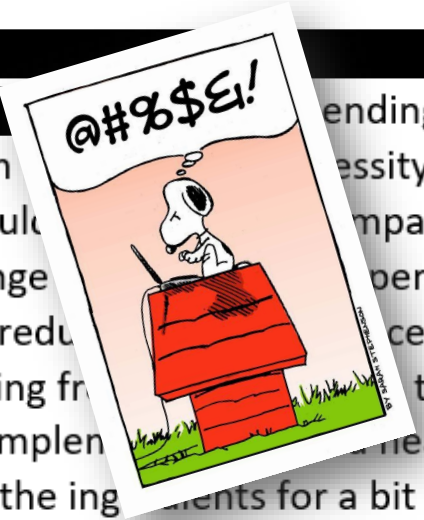
Do not think twice about reaching out to us. Our company is very happy to assist you. You're able to discover all of our contact information on your personal page or the mobile app.

Disclaimer: This email and its content are private and intended solely for the addressee. Please notify the sender in case you've received this email by mistake or delete it.

From: [Redacted]
Sent: Friday, April 10, 2020, 11:32 AM
To: Vaughn Manning
Subject: RE: Phishing test response

Hi Vaughn,

[Redacted]
[Redacted] ending out
[Redacted] necessity. Click on
[Redacted] company. Thank
[Redacted] perfect storm
[Redacted] concern's about
[Redacted] that all of
[Redacted] healthcare
[Redacted] with its stimulus and we have the ingredients for a bit of panic.



We appreciate your support! Thanks, [Redacted]

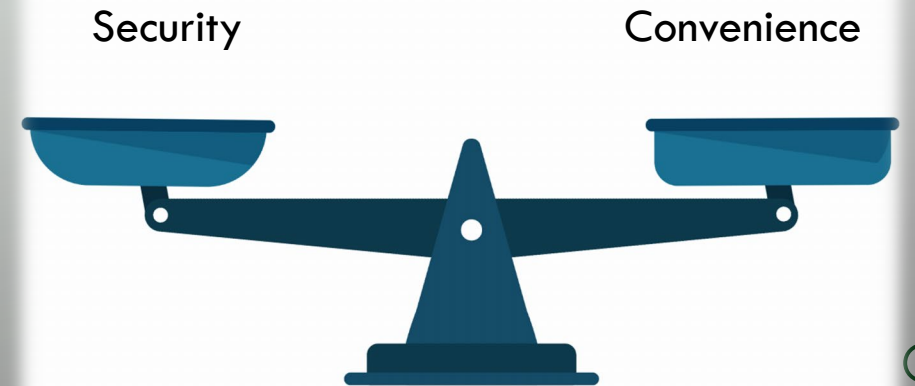
UGH, NOT ANOTHER CYBERSECURITY THING

- Lots of good reasons why people do cybersecurity poorly
- Information overload, analysis paralysis, sunk cost fallacy...
- The hardest part of doing something new is getting started
 - Candid and open questions with someone who understands it
 - Especially if they can show me



UGH, NOT ANOTHER CYBERSECURITY THING

- Cyber Wellness at home and at work
 - How does a mechanic treat their own car?
- You only need to know one password
 - Or, how to use a password manager
- Give a person a phish, tricked for a day
 - Teach a person to phish, and avoid the hook
- DOL on cybersecurity best practices
- Q&A (use chat along the way!)



@ HOME – BROWSER



Firefox > Edge > Chrome
(Mozilla) (Microsoft) (Google)



• > Google/Bing

DuckDuckGo.

• Ad-blocker:  uBlock Origin

• Password Manager:



• 3rd-party cookies, Do Not Track, HTTPS-only, DNS over HTTPS, oh my!

Cookie Preferences ...

Pocket's Cookie Settings

Necessary Cookies

Analytics Cookies

Personalized Advertising Cookies

Pocket's Cookie Settings
Pocket's **default** cookie settings are:
Necessary cookies - on
Analytics cookies - on
Targeting cookies - off


You can change your preferences by navigating to the categories on the left.
[More information](#)

Confirm **Reject All** **Allow All**

@ HOME – CELL PHONES

- iPhone and Android are both good!
 - iPhone: automatic, ecosystem lock-in, closed source, blue bubbles!
 - Android: as good as you make it, open source, green bubbles ☹️
 - Apple is better than Google at protecting user privacy, but is more anti-competitive
- Firefox with [uBlock Origin](#) or [AdGuard](#)
- Monitor app permissions. Re-install if unsure.
 - Replace apps with mobile websites
- Update OS and apps as soon as available
- Mobile hot spots > public Wi-Fi

@ HOME - MISCELLANEOUS

- VPN? Sure, for changing geo-location and privacy from ISP
 - most security issues are solved by  <https://www>.
- “Personalized” = tracking, look for ways to opt out
- <https://myactivity.google.com>
 - Delete activity older than 3 months
- <https://haveibeenpwned.com>
 - Check if your email has been listed in a breach
 - Create a spam email and use services like Firefox Relay
- And now, more than you ever wanted to know about passwords



PASSWORDS

- A good password has high “entropy”
- Length is the key to entropy
- Character set is next most important

- Upper, lower, number, special

- $26 + 26 + 10 + 12 = 94$

- AAAA = 26 possibilities for each character

- $26 * 26 * 26 * 26 \rightarrow 26^4 = 456,976$ combos

- Aa@8 $\rightarrow 94^4 = 78,074,896$ combos (170x)

- AAAAAA $\rightarrow 26^6 = 308,915,776$ combos (3.96x)

- Aa@888 $\rightarrow 94^6 = 689,869,781,056$ combos (2233x) (1.51M x)

Which password is better?

g1#T+sWv4rb	AAAAAAAAAAAAAAAA
-------------	------------------

5 lowercase	0 lowercase
-------------	-------------

2 uppercase	16 uppercase
-------------	--------------

2 number	0 number
----------	----------

2 special	0 special
-----------	-----------

11 characters	16 characters
---------------	---------------

72.1 bits	75.2 bits
-----------	-----------

**WARNING:
MATH**

YOU SHOULD ONLY KNOW ONE PASSWORD

- The master password to your password manager!
 - (and another one for work, where your IAM uses an IdP to SSO via SAML)
- Password managers have a learning curve
- The hardest part is getting started
- So let's do that together!



Start browsing or.

Express yourself by customizing Microsoft Edge with themes

Themes let you colour your browser to match your style. Choose from a number of options on the right.

Next



Overall appearance



System default

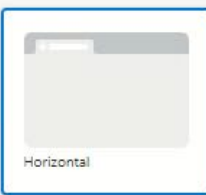


Light

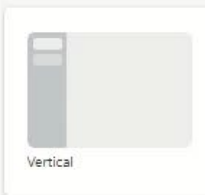


Dark

Tab layout



Horizontal



Vertical

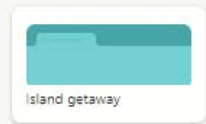
Pick a theme



Default



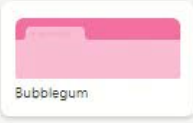
Icy mint



Island getaway



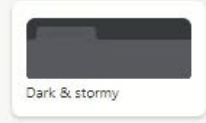
Silky pink



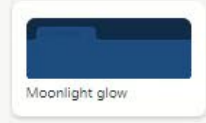
Bubblegum



Sunny day



Dark & stormy



Moonlight glow



NEW: Balancing Security and Innovation in the Age of

bitwarden Personal Business Developers Download Pricing

Bitwarden Browser Extension

Learn how the Bitwarden browser extension makes digital life easy, and explore more [download options](#) for all devices and browsers. Still need an account? [Sign up here](#)

[Sign up for free now](#) [Download options](#)

LOGINS 0

There are no logins available to auto-fill for the current browser tab.

[Add a login](#)

Tab Vault Send Generator Settings

More download options

You can access your Vault from anywhere in the world at vault.bitwarden.com. You can also [download and install](#) Bitwarden on any desktop, device, and browser.



[Download Logos](#)



Set your password

iczojrxob@mozmail.c

[Change email](#)

How old are you?

[Why do we ask?](#)

Get more from Mozilla:

- Security & privacy news and updates
- Early access to test new products
- Help keep the internet healthy

Create account

or

Continue with Google

Search vault

LOGINS 1


accounts.firefox.com
iczojrxob@mozmail.com

accounts.firefox.com

Tab Vault Send Generator Settings


Microsoft Wallet

- Payment methods
- Passwords**
- Personal info
- Show more
- Settings



Save time and money when you shop with Wallet
Keep your payment details safe and get Cash when you purchase online with a Microsoft a

Passwords










Scan the QR code to view and manage pa
Easy access to all your digital assets on the Edge

Search passwords

Password check

245 sites and apps

-  aa.com 3 accounts >
-  addwish.com 2 accounts >
-  ally.com >
-  amazon.com 2 accounts >
-  americanexpress.com 3 accounts >

Satisfied with Wallet?  

Search vault

TYPES 4

- Login 345 >
- Card 0 >
- Identity 0 >
- Secure note 0 >

FOLDERS 0

- No folder 345 >

TRASH 5

- Trash 5 >

Tab Vault Send Generator Settings



Set your password

iczoyrxob@mozmail.com

[Change email](#)

Password

Repeat password

How old are you?


[Why do we ask?](#)

Get more from Mozilla:

- Security & privacy news and updates
- Early access to test new products
- Help keep the internet healthy

Create account

or

 Continue with Google

Password requirements

- ⚠ At least 8 characters
 - Not your email address
 - Not a commonly used password
- 🔒 Stay safe — don't reuse passwords. See more tips to [create strong passwords](#).

CYBER WELLNESS – PASSWORD MANAGER

1. Install a browser extension/add-in
 - My IAM SSO might I-D-what now?
 - Okta, Onelogin, Entra ID
 - Authenticator apps like Duo, Authy, Google/Microsoft Authenticator
 - Avoid SMS and push notification MFA
 - Passwordless auth or “passkeys” is the future, but it’s not ready yet
2. Export passwords from your current browser(s)
3. Imported them to the password manager
4. Told the browser to stop helping

@ WORK – EMAILS

- The Three Yesses
 - Was I expecting this email?
 - From this person?
 - At this time?
- If you don't have all Three Yesses, think carefully before proceeding
- Use a second channel to verify unusual requests
 - Telephone, alternate email, a different person not CC'ed
 - Use your address book, not the email signature
- Report to your IT group! You probably have a button in Outlook.

@ WORK - ANATOMY OF A PHISH

- Next-gen attacks are happening now
 - AI-enhanced phishing campaigns
 - Proxy to steal session token
 - Commoditized malware
- Password cracking happens offline
- IAM SSO makes strong MFA important
- What is the dark web? Deep web?
 - Tor browser, onion links
 - Access brokers, ransomware-as-a-service

Evilginx Mastery Training Course

If you want everything about reverse proxy phishing with Evilginx - check out my [Evilginx Mastery](#) course!



Learn everything about the latest methods of phishing, using reverse proxying to bypass Multi-Factor Authentication. Learn to think like an attacker, during your red team engagements, and become the master of phishing with Evilginx.

Grab it here: <https://academy.breakdev.org/evilginx-mastery>

DOL'S NEW CYBERSECURITY GUIDANCE

- ERISA, 1974. Cybersecurity guidance, 2021.
- Tips for Hiring a Service Provider
 - ISO 27002, NIST 800-53
 - Right to audit
 - A past breach is not a disqualifier
- Cybersecurity Program Best Practices
 - Considerations that marketing, legal, sales, manufacturing, etc don't have:
 - ERISA, HIPAA, HITECH, GLBA, SOX, PCI DSS... ~~None~~
 - IT either has a framework you can join, or is looking for a partner
- Online Security Tips

THANK YOU



Vaughn Manning
Senior IT Security Engineer at
Transwestern



Don't Forget to Self-Report Your Credit

- Today's session qualifies for 1 Credit
- www.ifebp.org/myprofile
and select the orange box

**Manage Your CEBS
Compliance Credits**



**Scan to
self-report CEBS
compliance credit
from today's
session!**

Join Us for Our Next Event!

- Next Webinar is Thursday, April 11
 - Managing Benefits in a Unionized Environment
- Visit our website: dfwiscebs.org
- Join online at www.iscebs.org/join



Scan to
self-report CEBS
compliance credit
from today's
session!