



Cyber Security Readiness for Small Businesses

Are you prepared? / Learn How to Save Your Small Business and It's Data

Hosted By: The Town of Trumbull in collaboration with the Trumbull Economic and Community Development Commission, Bridgeport Regional Business Council, Kyber Security, CT Small Business Development Center, Crown Castle, & Gallagher Insurance



Insurance | Risk Management | Consulting



Agenda



April 27, 2023 • 8:00a.m. – 10:00a.m.

Emcee: Rina Bakalar, Director of Economic & Community Development

8:00am Registration and Breakfast

8:30am Opening Remarks

Rina Bakalar, Economic & Community Development Director

Lynn Souza, CEO Kyber Security

8:45am Presentation: State of Cyber Security

Bob Thomas, CISO of Kyber Security

9:00am Presentation: Employee Awareness

Massimo Mallozzi, VP of IT for Paris Baguette

9:15am Panel Discussion: Cyber Insurance • Ransomware • Best Practices

Ryan Kelly, of Gallagher Insurance

Bob Thomas, CISO of Kyber Security

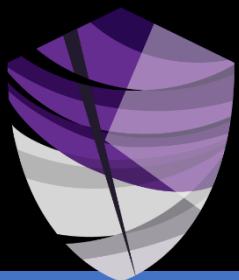
Valeria Bisceglia, Business Advisor for CT SBDC

9:40am Close Out Discussion & Takeaways

The State of Cyber Security for SMBs

SMBs are under attack.
Protect your organization!

*Presented by: Bob Thomas,
Chief Information Security Officer of Kyber Security*



Complexity of a modern small business

- Email
- Mobile devices
- Corporate website
- Social media
- Ecommerce systems
- Online banking
- BYOD and office policy
- Network management
- Backup and remote access



Small Business, Big Impact

Why put your already limited resources into preparing for and protecting against cybersecurity attacks?

Vulnerability

Attackers see small businesses as easy targets

Business Costs

Attacks can be extremely costly and threaten the viability of your business

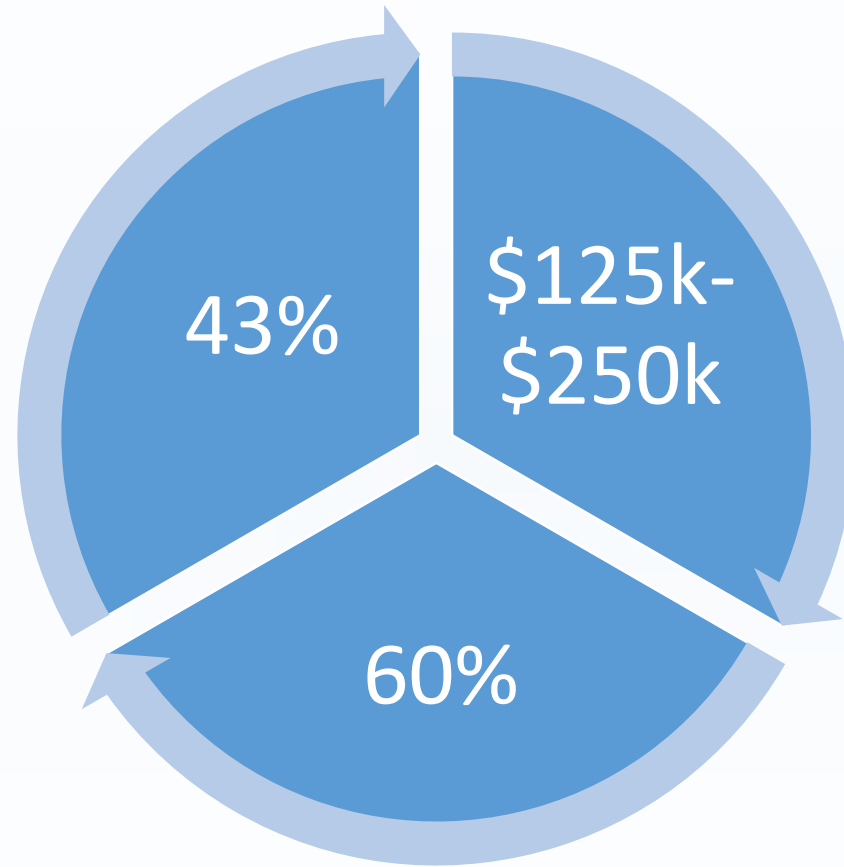
Reputation

Customers and employees expect and trust you to keep their information secure



SMB Breach Stats

Percentage of
cyber attacks
against SMBs



Average cost of
cyber attack
against SMBs

Percentage of SMBs that go out of
business after cyber attack



What is a Data Breach?

- **A data breach exposes confidential, sensitive, or protected information** to an unauthorized person. The files in a data breach are viewed and/or shared without permission.
- **Anyone can be at risk of a data breach** — from individuals to high-level enterprises and governments. More importantly, anyone can put others at risk if they are not protected.



What Kinds of Information are at Risk?

- Personal Identifiable Information (PII)
- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)



Consequences of a Data Breach

- Financial Loss
 - Delay in operations
 - Steep fines
- Loss of Business
 - Weakened business brand
 - Client mistrust
- Legal Issues Can Impact Your Firm
- Damaged Business Reputation



Common Breaches

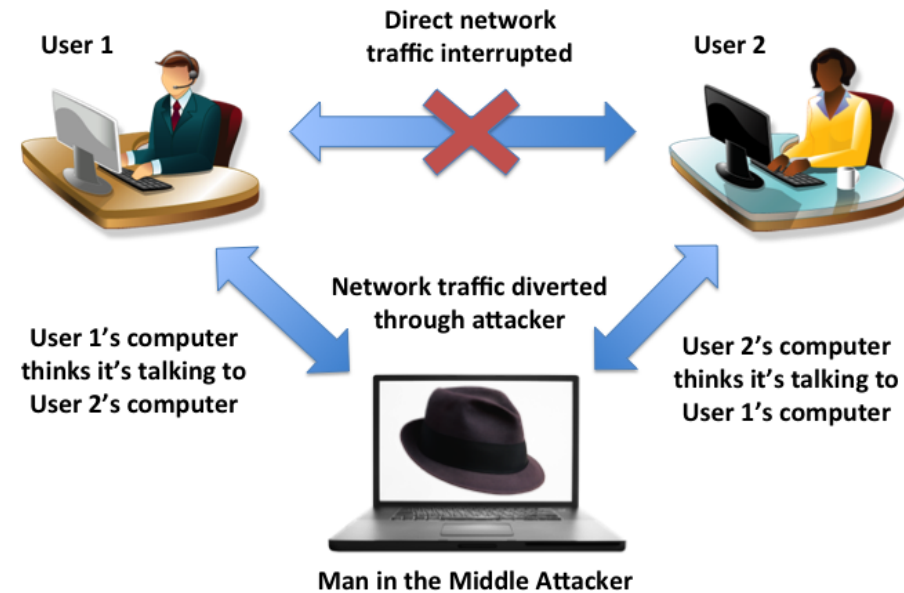
- Business Email Compromise
- Ransomware
- Distributed Denial of Service Attacks
- Imposter Scams



What is Business Email Compromise?

- An attacker obtains access to a business email account and imitates the owner's identity, in order to defraud the company and its employees, customers or partners.

- AKA “man-in-the-email attack”



Ransomware

When criminals hack your computer or network, lock you out, and demand a ransom to let you back in



Distributed Denial of Service

DDoS are attempts to make a network resource unavailable to its intended users



Disguised a regular traffic,
DDoS attacks are complex and difficult to detect

By overwhelming a web site/server/network using botnets

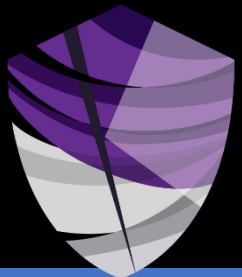
Common Scams

- **Apartment Rental Assistance**
- **Fake Microsoft Employees**
- **Hurricane Donations**
- **Google Voice Scam**
- **CEO Impersonation**



CT Data Law

Cybersecurity Safe Harbor (HB6607)



Cybersecurity Safe Harbor (HB6607)

- **CT is the 3rd state** to institute the following type of law (Ohio & Utah are the others).
- **Offers protection from CT Supreme Court assessing punitive damages if the organization has:**
 - Created, maintained and complied with a written cybersecurity program that contains administrative, technical and physical safeguards for the protection of personal or restricted information
 - Conformed to an industry-recognized cybersecurity framework:
 - PCI DSS
 - ISO 27000-series
 - HIPAA
 - Gramm-Leach-Bliley Act
 - NIST CSF



Looking for a **Defense in Depth** Strategy



Penalties for Violations

Criminal

- 1st offense: \$100 per willful violation
- 2nd offense: \$500 per willful violation
- 3rd and subsequent offenses: \$1,000 and or 6 months imprisonment

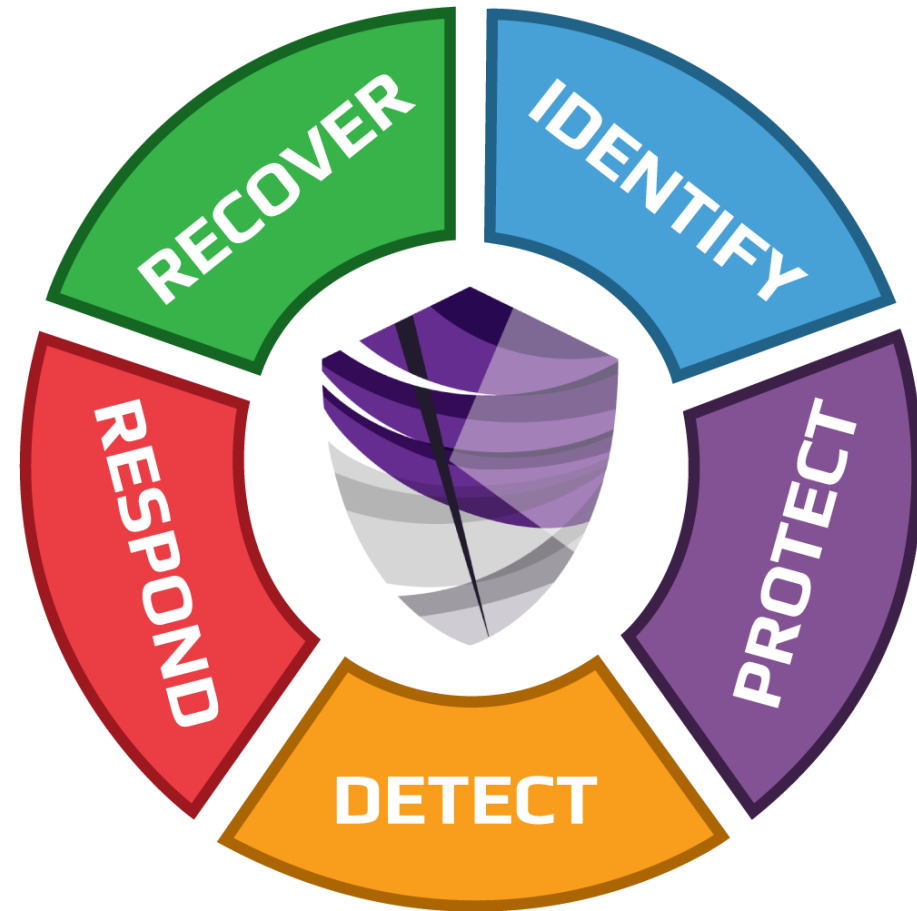
Civil

- \$500 per willful violation, to a maximum of \$500,000 for any single event.

**Penalties shall be deposited into the CT privacy protection guaranty & enforcement account.*



NIST Cybersecurity Framework



What is the NIST Framework?

- A voluntary set of best practices and guidelines.
- Designed to measure business cybersecurity posture relative to the threats they face.
- Applicable to all organizations regardless of industry and size.
- Intended to be the basis for a comprehensive cybersecurity program which may include things you are already doing today.
- Will provide a **common language for managing cyber risk** between IT and business management.



BREAKING DOWN THE NIST Cybersecurity Framework

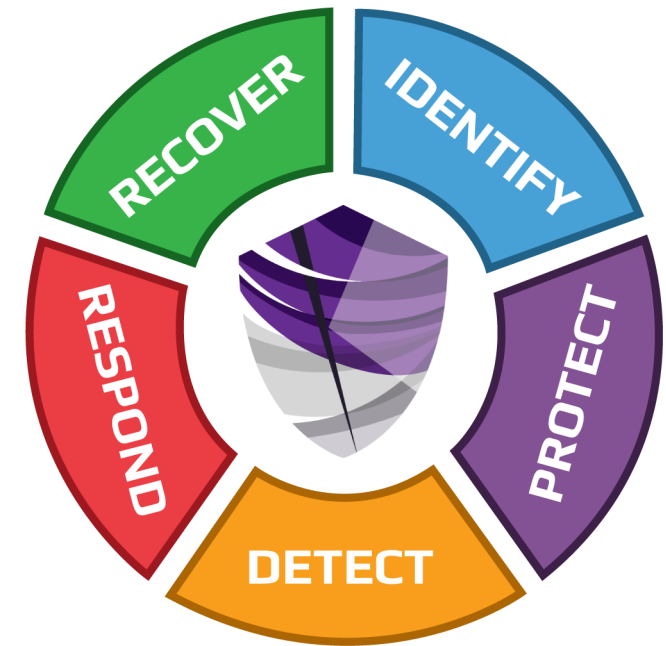
Identify – prioritize cybersecurity efforts consistent with business needs.

Protect – prevent cybersecurity incidents and limit the impact of potential incidents.

Detect – establish timely discovery of cybersecurity events.

Respond – contain the impact of cybersecurity incidents.

Recover – sustain timely recovery to normal operations to reduce the impact from a cybersecurity incident.



Lessons Learned

- SMBs are under attack!
- Common scams can cripple your organization
- 60% of SMBs who suffer an breach go our of business
- Follow a framework such as NIST CSF to protect your organization and avoid fines



Special Offer



No-Cost Compact NIST Cyber Security Framework Assessment

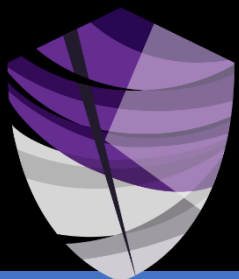
Sign Up



Here's What You Can Expect From A CSF Assessment:

- Understand your organizations gap with core components of the NIST CSF
- Obtain immediately actionable information for how you can better secure your business
- Learn how you can improve the overall cybersecurity posture of your organization

[Kybersecure.com/csf-assessment](https://kybersecure.com/csf-assessment)



Thank you!

Tell us what you think!



www.kybersecure.com
marketing@kybersecure.com



Employee Awareness

*Presented by: Massimo Mallozzi, VP of Information
Technology for Paris Baguette America*



How does Security Awareness Training help individuals?

It gives you the know-how to stay safe from cybercrime...

AT HOME

- Protect your identity and personal data from theft and fraud
- Secure your devices against viruses and malware
- Keep yourself and your family safe from hackers and spies

AT WORK

- Prevent corporate network infections
- Stop business email compromise
- Keep critical business data safe

How does Cybersecurity Awareness Training help businesses?

Reduce Breaches and Infections

- Improve mindset and behavior
- Create a sense of shared security responsibility
- Reduce over-reliance on technology

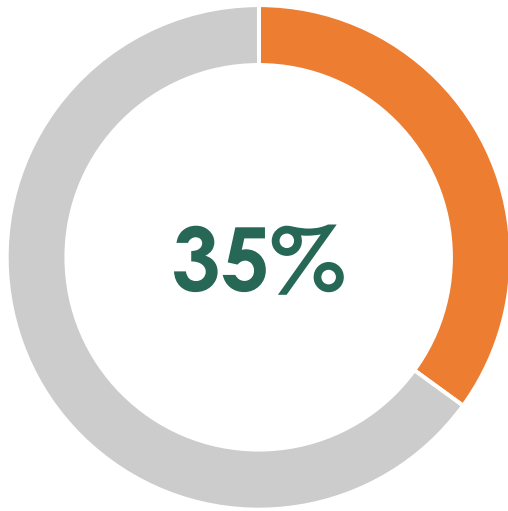
Meet Regulatory Requirements

- Implement best data governance practices
- Meet compliance objectives
- Implement affordable cyber-insurance

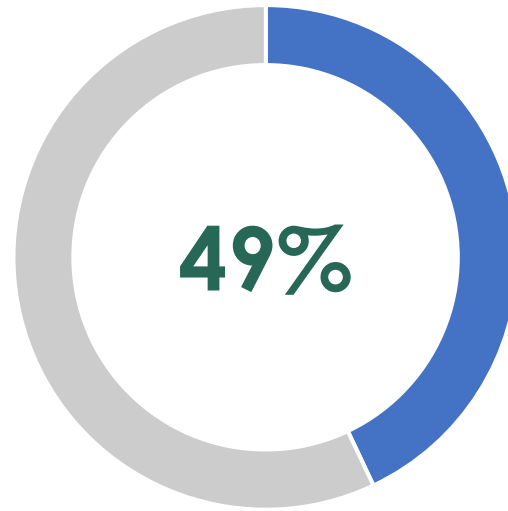
High Return on Security Investment (ROSI)

- Fewer infections
- Lower clean-up/support costs
- Stronger security posture
- Higher productivity
- High security benefit vs. operational costs

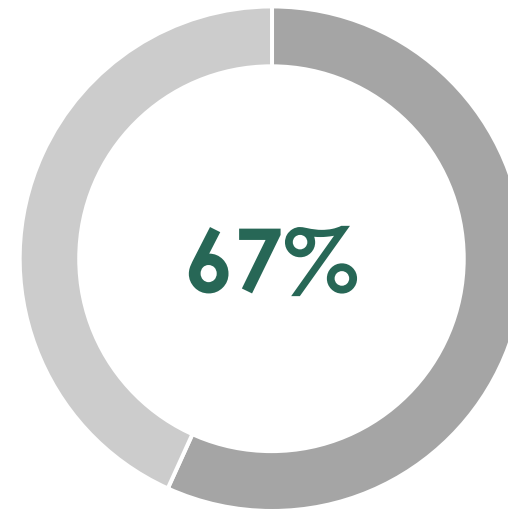
But people know better, right?



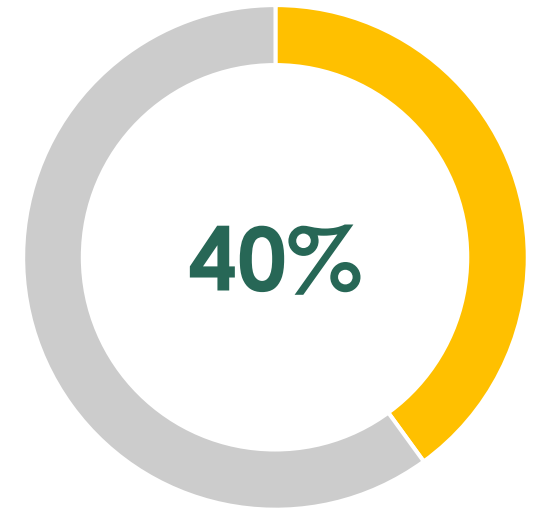
Of workers who know they've been hacked don't bother to change their passwords afterward¹



Of employees admit they click links in messages from unknown senders during work¹



Of workers are sure they've received at least one phishing email at work¹



Of those who received a phishing email, ~40% didn't report it

BEC comprised 37% of all losses last year

¹ Webroot Inc. "Hook, Line, and Sinker: Why Phishing Attacks Work." (September 2019)

Phishing



When Scammers **fool you** to think they are someone you trust in order to make you **do something**.



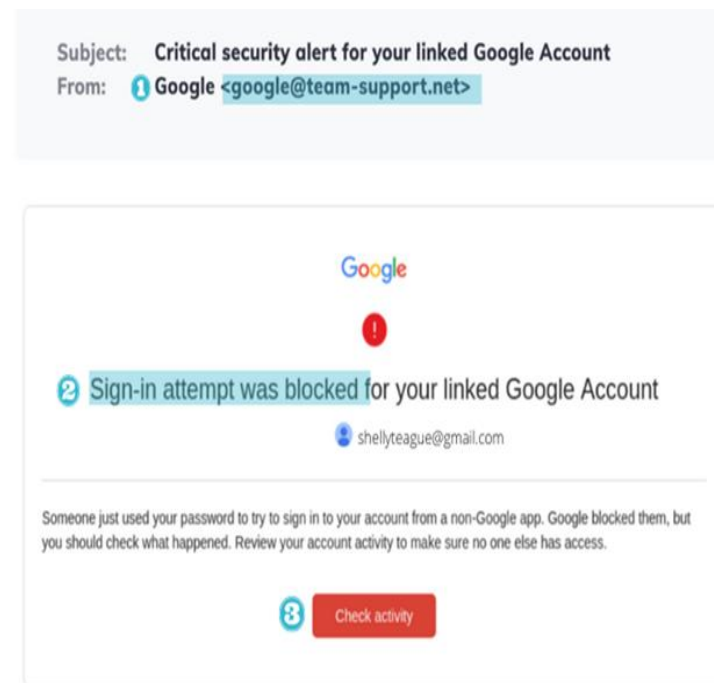
The email is disguised and looks like an email from a **reliable source**, but in reality, it's a link to a malicious site.

Types Phishing Scams You **Should Be Aware of**

Email Phishing Scams

It may look like an email from your bank, PayPal, Google, Amazon, or even your CFO or CEO.

- 1 Sender Email**
Email domain is not official @google.com
- 2 Alert for immediate action**
Scams push for quick action under emotion. Instead, pause and look for red flags.
- 3 Redirect**
Hover over button reveals bit.ly link instead of official site



You received this email to let you know about important changes to your Google Account and services.
© 2021 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Spear Phishing/Whaling Scams

Scams that target individuals or high ranking members of an organization (whaling).

They have researched you, they know your family members, where you work, your boss and your employees. The chances of fooling you are higher.

- 1 Account payroll question External Inbox x
- 2 Ann Carlisle <homeofficeinternal19@gmail.com> Fri, May 27, 3:31 PM (3 days ago) ☆ ↶ ⋮
to me ▾
- 3 Hello April,
- 4 Please I would like to change the account on my payroll to a new account. Would it be effective next payday?

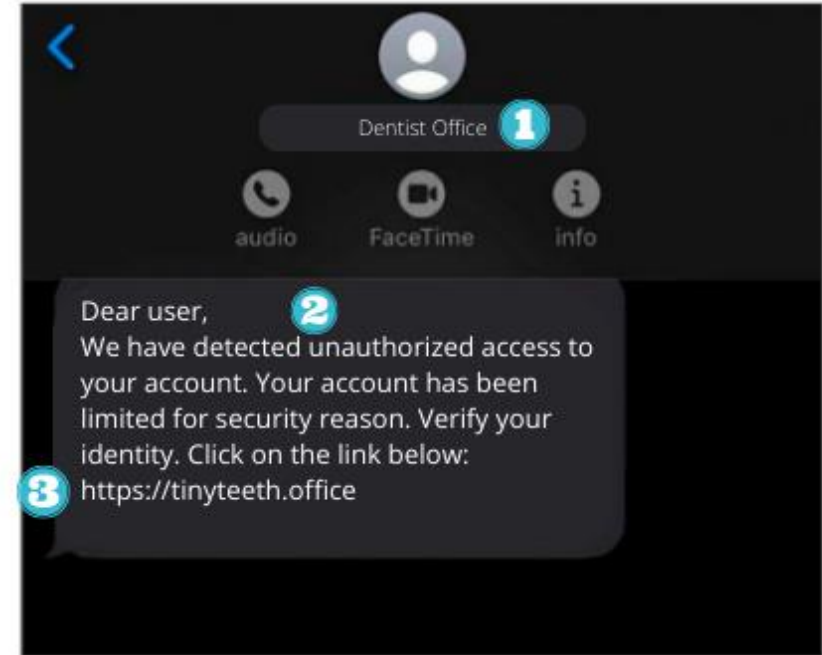
Thanks.
- 5 Ann Carlisle
Customer Success Specialist

- | | | |
|--|--|--|
| 1 Subject line:
Sense of familiarity | 3 Greeting:
Personalized | 5 Correct Job Title
Contact name has correct job title. Spearphish attackers do their homework to look as legit as possible. |
| 2 Sender Name & Email:
Sender Name is trusted name in Contacts. Email is generic Gmail instead of company email. | 4 Message:
Starts a conversation to build trust before a phishing link is sent or action is requested. | |



Smishing Scams

These are text message phishing scams. Criminals know people respond to text and instant messages faster than email.



1 Lookalike Contacts
Generic Contact Name is similar to Trusted Contact role.

2 Message
Message conveys sense of urgency and fear.

3 Lookalike URL
Scammers buy lookalike domains similar to, but different from, the real company site.

Google Search Scams

You may be surprised, but some of the top search results in Google are phishing links.

Scammers also invest in search engine optimization and work hard to rank their scam sites in the top search results.

1 Search Result Shows Brand

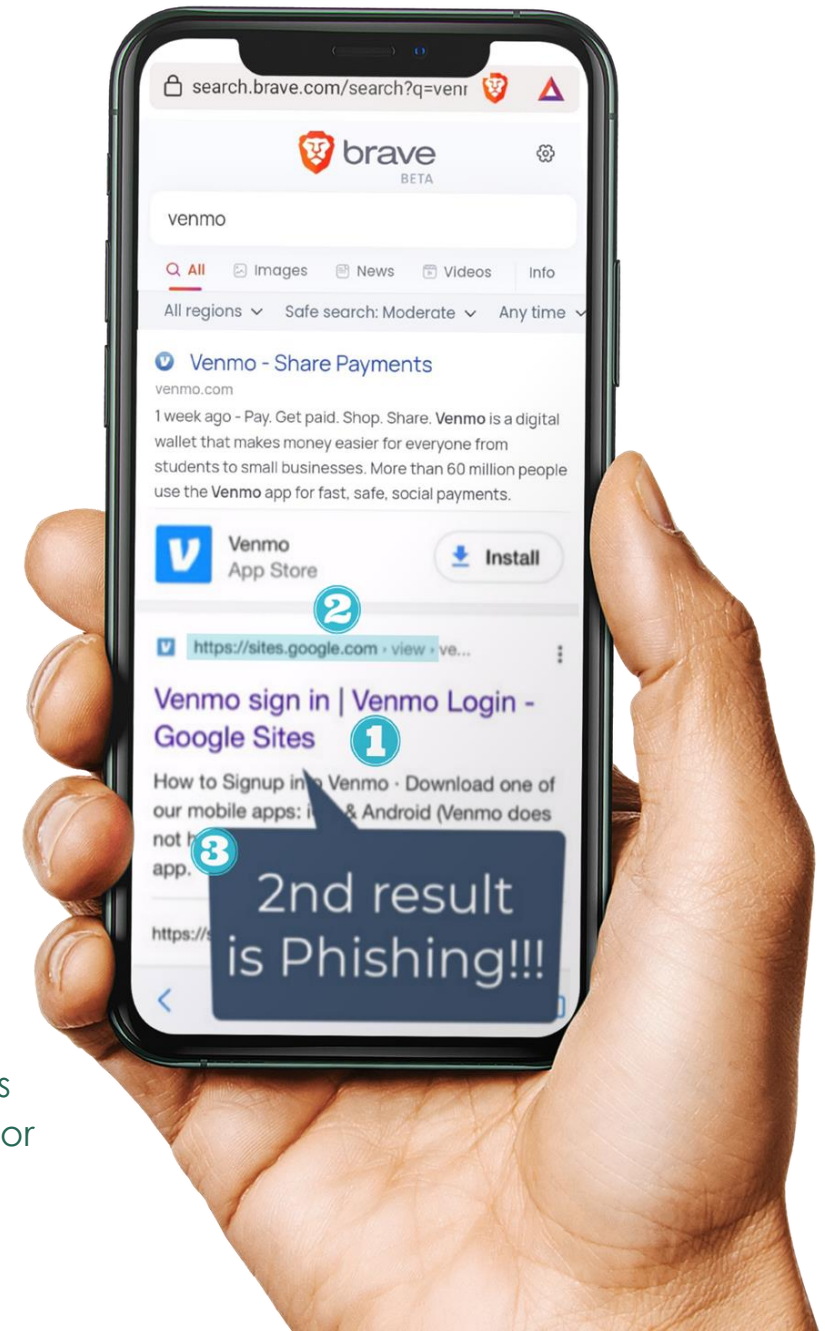
Title displays correct brand name

2 URL Mismatch

Title says Venmo but URL is a generic sites.google.com

3 2nd Result for Organic Search

Even top search results can be manipulated for fake sites



Social Media Scams

Social media is full of fake accounts.
It could also be a fake account with the same name and photo as one of your real friends that will later try to scam you.

1 Known Contacts
Friend requests from people already connected with you.

2 Inactive Following
Zero or low followers is a flag especially if you know these people have been active a long time.

3 Odd Characters in Handle
Both use name of the Contact with minor variation to try and avoid notice '_.' or '._'

QR Code Scams

Who thought a QR code could be dangerous?

They are everywhere, especially in restaurants. Criminals can place their own sticker over the legitimate one. So that when you scan it, you will be redirected to a fake site.



Vishing Scams

Vishing (voice phishing) is a type of phishing attack made over the telephone.

Scammers can spoof a phone number that looks identical to a known number, like your bank.



Trusted Brands

Numbers for personal and commercial contacts can be spoofed.

What Helps Protect You From Phishing Attacks?

- If it's urgent, don't let the emotions cloud your judgment
- Call and verify! - Verify that you are talking to the correct person
- Check the address - Always check the email address and URL for spelling mistakes – Not just the name!
- Enable Multi-Factor Authentication if available
- Look at the style of the message
- Ask questions

How long will it take to crack your password?

7 characters	1 minute
8 characters	1 hour
9 characters	3-4 days
10 characters	7 months
11 characters	40 year
12 characters	2000 years

Passwords include - Lowercase, Uppercase and Numbers

PASSWORD

How to create a strong Password:

Passwords need to be **long**!

- Use a phrase (**NO** personal info like your name or B-Day)
- Avoid shoulder surfers and enter your credentials carefully! If a password is entered in the username field, those attempts usually appear in system logs.

❖ **Don't** reuse passwords!

How to create a strong Password:

- A familiar quote can be a good start:
- Using the organization standard as a guide, choose the first character of each word:

"LOVE IS A SMOKE MADE WITH THE FUME OF SIGHS"
William Shakespeare

- LIASMWTFOS
- Now add complexity the standard requires:
 - L1A\$mWTFOS (10 characters, 2 numerals, 1 symbol, mixed English case: password satisfies all 4 types).
- Or be more creative!

HOWEVER....

11 BILLION Accounts were stolen from hacked sites and apps.

So even if you have a **STRONG PASSWORD**, it may still not be enough.

You can check if yours was leaked at www.haveibeenpwned.com

And That is Why...

... **Multi-Factor Authentication is critical**

MFA helps to **protect your account** if your password was stolen or leaked in a data breach.



What type of Multi-Factor Authentication to use?

- Text based (SMS) is most commonly used, but the least secure
- Authenticator apps like Google or Microsoft Authenticator are more secure

How to avoid getting hacked on public Wi-Fi:

- If you have the option to **use** your **mobile data plan**, that's better than public WiFi
- Criminals often setup hotspots with fake Wi-Fi Names, so **ask** an employee for the **official Wi-Fi Name**
- Enable the Firewall on your device and **use a VPN**
(Try to avoid Free VPN's - some are owned by criminals)

Ransomware

When criminals hack your computer or network, lock you out, and demand a ransom to let you back in.



How to Avoid Ransomware ?

- **Don't download** files from random websites
- **Beware** of phishing emails with attachments
- **Don't use** your business email or password for personal stuff
- **Don't store** passwords in text files or spreadsheets

What is Wire Fraud?

It's when you're tricked into wiring money to a fraudulent bank account. For example:

An urgent request to wire money from a criminal who impersonates your CFO through hacking your CFO's email account.

- They hacked one of your vendors and sent you an invoice with fake bank information.
- If you're tricked into wiring money to a fraudulent bank account, the bank may not be able to help. After all, it's **you who transferred the money**, not the criminal.

How to Avoid Wire Fraud:

- **Call and verify** any request for funds transfer
- **Call a known number** that you used before or from the vendor management system
- **Always verify** bank information matches the one you have on file
- **Call and verify** any request to change info on file, like phone number, address or bank account information



Panel Discussion

Moderated by Mike Giuffrida, President Kyber Security

Speakers

Ryan Kelly, Risk Management Advisor

Bob Thomas, Chief Information Security Officer

Valeria Bisceglia, Business Advisor





NO-COST RESOURCES FOR CYBERSECURITY

Valeria G. Bisceglia

Education & Training Programs Advisor,
CT Small Business Development Center



DATA ASSURED PROGRAM

Turnkey solution allowing cybersecurity education for all small businesses.



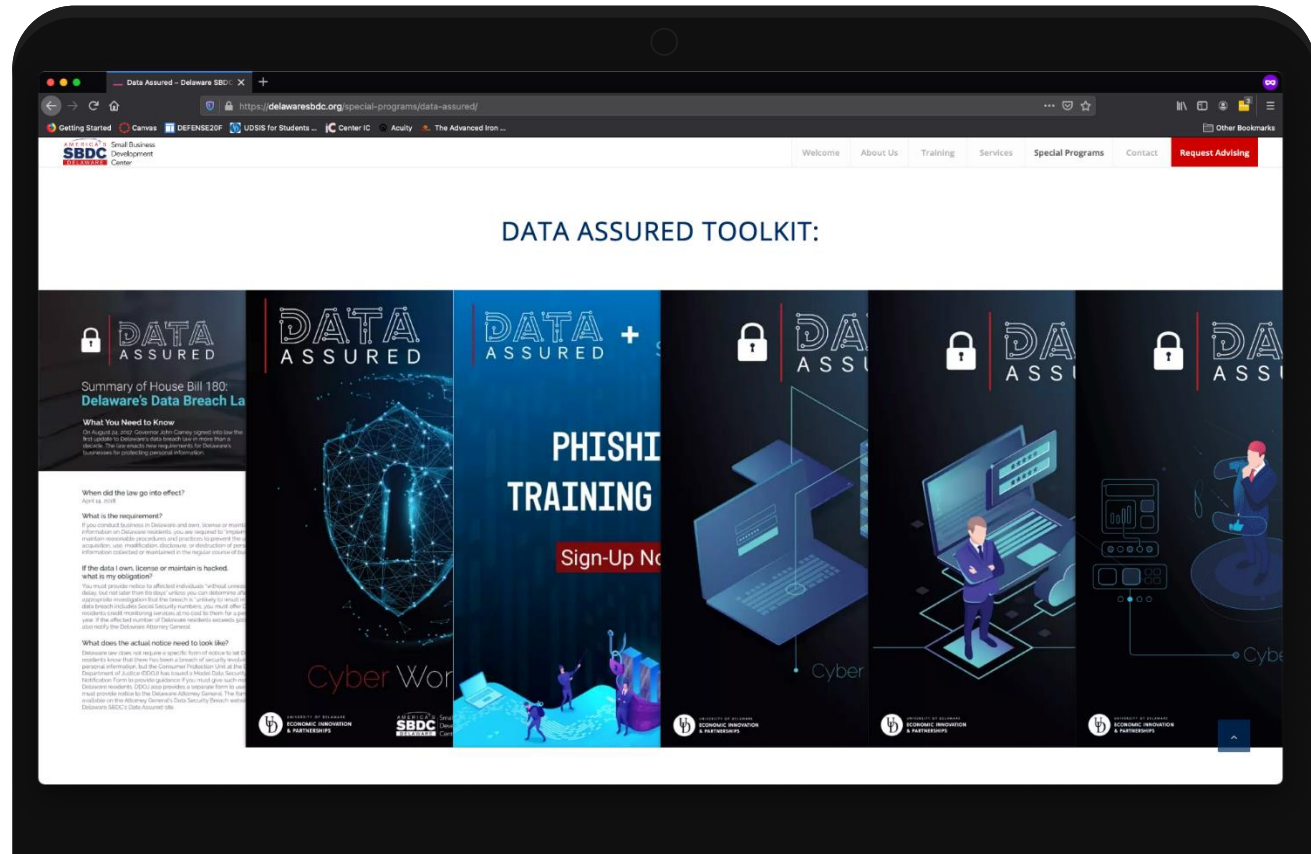
Award-winning Cyber Workbook

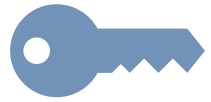


Cybersecurity One-Pagers



Connecticut SBDC Support





TEST YOUR PASSWORD SECURITY

How Secure Are Your Passwords?

TEST YOUR PASSWORD SECURITY BY
USING THIS FREE, SECURE TOOL:

<https://www.security.org/how-secure-is-my-password/>



HOW PASSWORD
LENGTH WINS
THE INTERNET

Passwords 102

1

Create
Original
Passphrase

Pizza is my favorite
food

2

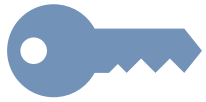
Ensure
Passphrase
Usability

Pizzaismyfavoritefood

3

Strengthen
Passphrase

P1ZZ4I5Myfav*r1teF**d



CHECK E-MAIL & PASSWORD COMPROMISE



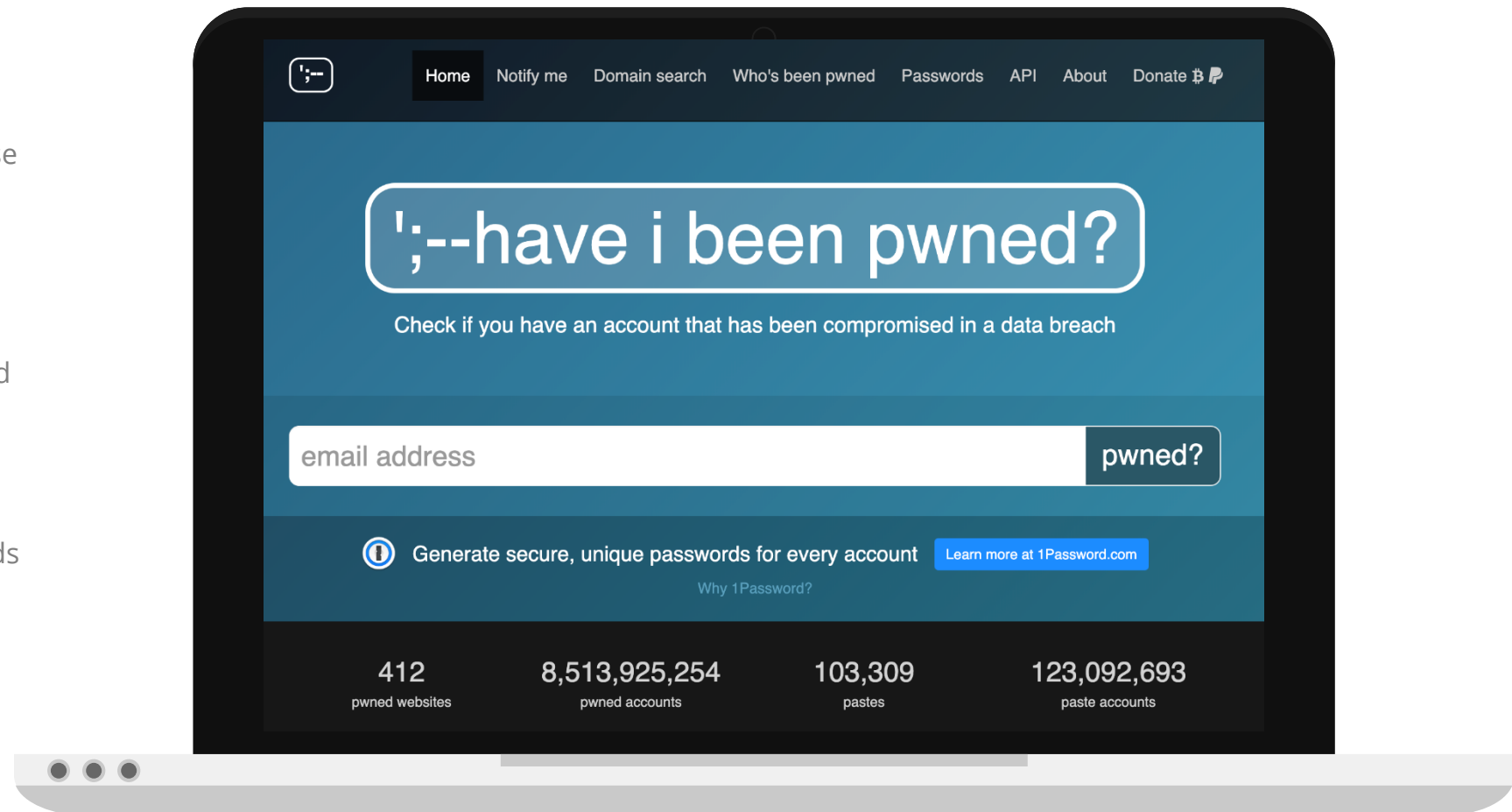
Email and password compromise check. Go to haveibeenpwned.com



Type in your email to see if that email address has been exposed in a data breach



You can also test your passwords as well and it will tell you if that password has ever been leaked





TEST YOUR PHISHING KNOWLEDGE



It is important to test yourself!
Hackers are getting smarter

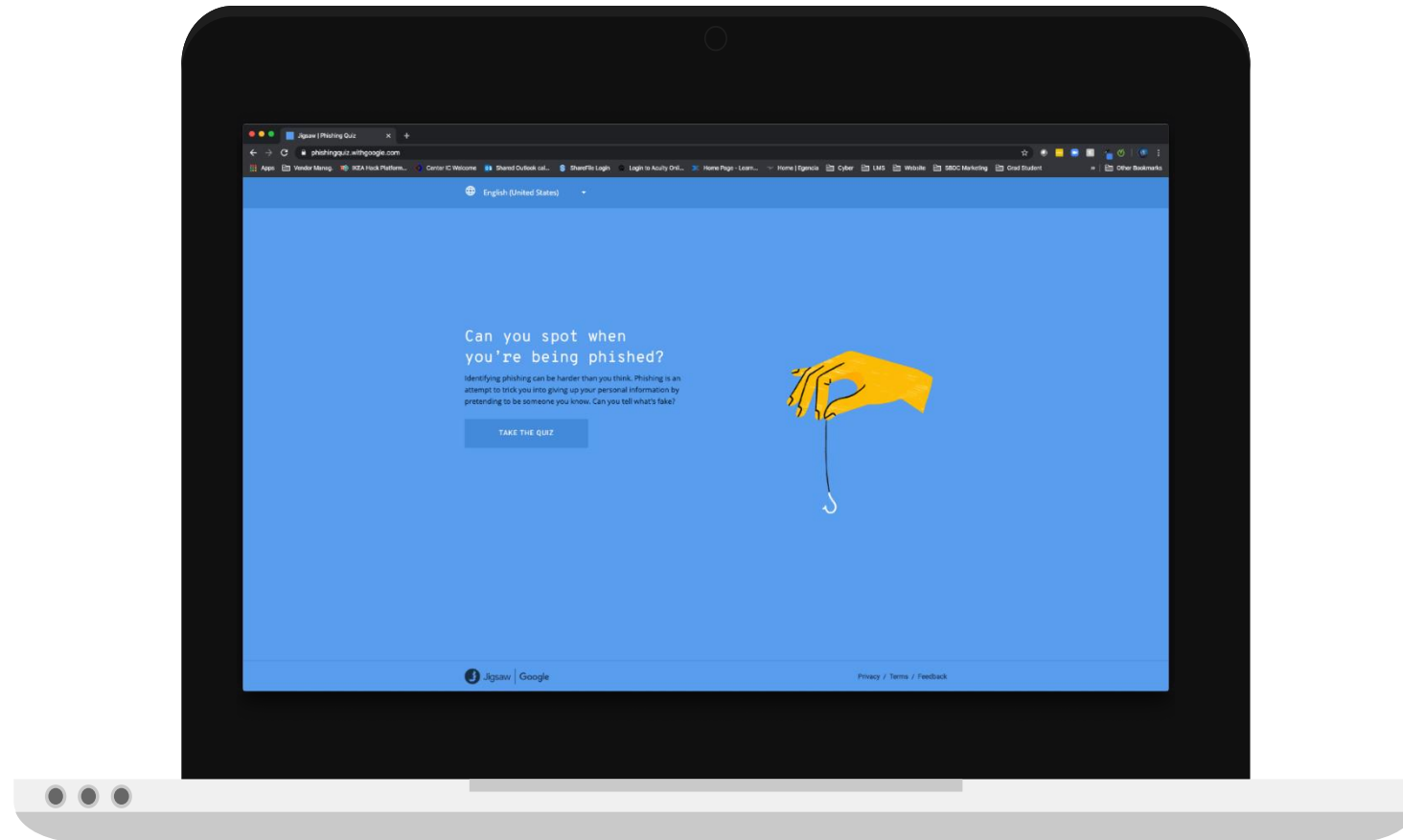


If you don't feel right about
an email delete it!



Test yourself at:

[https://phishingquiz
.withgoogle.com](https://phishingquiz.withgoogle.com)



GET CONNECTED

✓ Request business advising support ctsbdc.uconn.edu

✓ Follow us    
@CTsbdc



Key Takeaways

Please see handouts included in event package

Cyber Do's & Don'ts
Cyber Solutions
Cyber Tips

Accessing Information From This Event:

Resources from this event will be posted on to the Town of Trumbull website:

<https://www.trumbull-ct.gov/345/General-Business-Advice-Technical-Assist>



Thank You To Our Partners:

