INQUISITIVEIT.COM

CHECKLIST - 20 things you need to do today

Help your clients avoid costly hacks, scams, and account takeovers with a hardened and dedicated “Investments Only” laptop for Individuals .

Talk to Inquisitive IT about Training and Vaultbook

Checklist

1. Start using **Passkeys and Security Keys** - These security keys can disrupt many different attack vectors.. Its also PASSWORDLESS and faster to log in.. WIN WIN!
2. **Password Managers** - create unique and complex passwords. Don’t let one breach affect all of our accounts. Start using a password manager and replace all passwords with randomly generated passwords. Examples include Apple Keychain, Google password manager on Chrome, 1password, Bitwarden
3. **Never click on links in your email or text. Always navigate directly to the web page from browser.**
4. Always **triple verify “out of band” on new ACH and Wire Instructions.** Cyber Insurers #1 LOSS. Be anxious and wear the tin hat when it comes to sending money to new places.
5. Make sure you and your **family’s social network’s are closed and audit your friends** to see if you accepted some that you do not know personally. Don’t overshare personal details. Post trips photos after and not during.. It lets attackers know you may not be home.
6. **Stop getting paper statements** from banks and financial institutions. You dont want to need a shredder.
7. Create **seperate email account for financial affairs vs personal..** Extra credit use a separate device.
8. **Utilize a managed browser** to prevent spoofed sites, malware execution, and more. This likely comes from a managed service like Inquisitive. Google Advanced protection is less effective, but strong defense. Inquisitive complies with CIS Standards for Chrome Browsers
9. **Update all devices and software ASAP**. It takes newly discovered attack vectors and vulnerabilities off the board.
10. **Dont use public wifi**. Use a hotspot. If necessary, use VPN
11. **Turn on credit card and bank text notifications** any time money moves.
12. **Set up legacy contacts** in Google, Apple, Microsoft, Amazon so that after death, access is passed accordingly
13. **Dont use USB ports to charge publicly**, use the 110v outlet

Stop Attacks

Ransomware

- Managed browser will not execute clicks on malware or phishing links
- Software and configuration vulnerabilities are continuously removed
- Screen out phishing emails

Identity Theft

- Continuous cleaning of personal identity with dark web scans and public search records (social media)
- Increased authentication protocols deter email takeover / phishing

Fraudulent Money Transfers

- Policy training and protocols to deter illegal money transfers
- Authentication, email security, and browser defenses to deter social engineering attacks

Account Takeovers

- Phishing resistant authentication deters account takeovers
- Intrusion detection
- Continuous Dark Web monitoring
- Unique and complex passwords via password managers and forced compliance
- Password compromise alerts

Contact Us

☎ **+551-751-0010**

🌐 **www.inquisitiveit.com**

Inquisitive IT

INQUISITIVEIT.COM

CHECKLIST - 20 things you need to do today

Help your clients avoid costly hacks, scams, and account takeovers with a hardened and dedicated "Investments Only" laptop for Individuals .

Talk to Inquisitive IT about Training and Vaultbook

14. Use a **VPN both outside the home and inside the home**. Its an extra level of protection if you network has been compromised.
15. **Set up a guest network on your home WIFI**, and put everything with exception of your phone and laptop on it. IoT devices should not share network with critical computing.
16. **Dark Web Scans** to see what data has been compromised and likely sold to bad actors. Google one provides them if you buy storage from Google. Get alerts when there is a leak.
17. **Pay for service to scrub your online history,** rotate passwords as well if found.
18. EDR - **Endpoint detection and response is the fire alarm** to catch suspicious activity on your laptop.. Likely provided by a provider.
19. **Turn off Weak Forms of MFA** (email backup, 6 digits codes, authenticator apps). Have two Fido 2 Keys
20. Make sure your **phone and laptop locks** after a short time period. We see devices unlocked and unattended.

Why Choose Us

Deep Industry Experience

Experience in Big4 Cybersecurity advisory to Fortune 500 companies and Federal Agencies

Willing to Manage Risks that Banks Won't Assist With

Large financial institutions are unwilling to roll their sleeves up and assist with securing the individual due to liability and regulatory hurdles including data protection

Vendor Agnostic and Flexible Deployments are Unique in the Market

Unlike traditional MSPs or MSSPs, We borrow practices from mature cyber programs including people, processes, policies, and custom technology where necessary

Stop Attacks

Ransomware

- Managed browser will not execute clicks on malware or phishing links
- Software and configuration vulnerabilities are continuously removed
- Screen out phishing emails

Identity Theft

- Continuous cleaning of personal identity with dark web scans and public search records (social media)
- Increased authentication protocols deter email takeover / phishing

Fraudulent Money Transfers

- Policy training and protocols to deter illegal money transfers
- Authentication, email security, and browser defenses to deter social engineering attacks

Account Takeovers

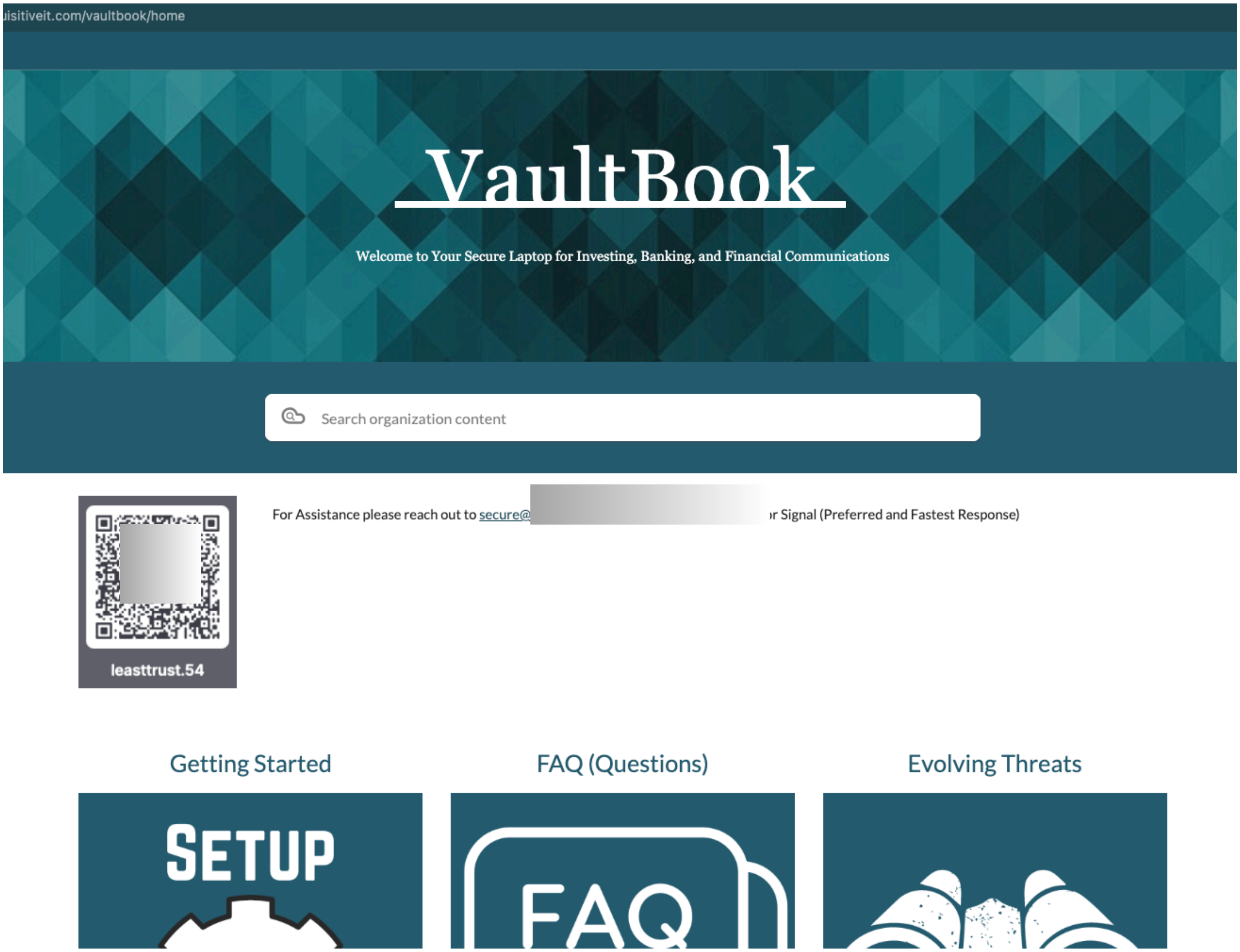
- Phishing resistant authentication deters account takeovers
- Intrusion detection
- Continuous Dark Web monitoring
- Unique and complex passwords via password managers and forced compliance
- Password compromise alerts

Contact Us

☎ **+551-751-0010**

www.inquisitiveit.com

VaultBook Landing Page and 24/7 Assistance



isitiveit.com/vaultbook/home

VaultBook

Welcome to Your Secure Laptop for Investing, Banking, and Financial Communications

Search organization content

[redacted]

leasttrust.54

For Assistance please reach out to secure@[redacted]r Signal (Preferred and Fastest Response)