



**PROCUREMENT AND  
ENFORCEMENT  
OF INTELLECTUAL PROPERTY**

**CISLO & THOMAS LLP**  
Attorneys at Law

**PATENT, TRADEMARK  
COPYRIGHT & RELATED  
MATTERS**

C&T Staff Training  
May 17, 2023 (acs)

## **CYBERSECURITY**

1. What is cybersecurity?  
Cybersecurity refers to the protection of data against unauthorized use or from criminals.
2. What is a phishing attack?  
A phishing attack is a type of social engineering attack that tricks users into clicking on an attachment or on a link, typically in an e-mail format.
3. What is a ransomware attack?  
Ransomware refers to malicious software that often blocks access to a computer or online portal unless a ransom is paid.
4. What is malware?  
Malware is also referred to as malicious software, which is used to infect a computer, network or website—this is often in the form of a virus, Trojan, or worm.
5. What is an Incident Response Plan?  
An Incident Response Plan acts as a helpful resource for you and your business in case there is a data breach or an incident. It provides a set of instructions and contacts for your staff members.
6. What is the California Consumer Privacy Act (CCPA)?  
The CCPA gives California consumers more control over the personal information that businesses collect about them.
7. What is the California Privacy Rights Act (CPRA)?  
The CPRA amends certain provisions and requirements of the CCPA and establishes the California Privacy Protection Agency to oversee the law.

## What does Cislo & Thomas, LLP do to protect our cybersecurity?

1. **Antropy, Inc:** Identify and assess cybersecurity risks and threats; identifying vulnerabilities will provide a framework to minimize the risks and effects of a cyber-attack.
2. **Staff Trainings and Email Alerts:** Prioritize employee training and awareness programs since the majority of cyber incidents are caused by employees inadvertently clicking on phishing e-mails.
3. **Duo Mobile and Company Platforms** (DropBox, Zoom, etc.): Use Two-Factor Authentication to provide an additional layer of security.
4. **AppRiver:** Utilize filtering tools to minimize the risk of phishing e-mails.
5. **Veeam Backup & Replication:** Backup data on a regular basis to prevent unnecessary loss.
6. **Webroot and Barracuda Networks:** Update operating systems and antivirus programs to enhance internal security mechanisms.
7. **Cybersecurity Insurance.**

## What should staff do to help prevent vulnerabilities?

1. Update your applications and computer.
2. Be aware of phishing scams.
3. Two-factor authentication.
4. Password security and difficult level.

## To learn more about cybersecurity and data privacy:

1. [Cislo & Thomas, LLP Webpage](#)
2. [Cislo & Thomas, LLP FAQ](#)
3. [Cislo & Thomas, LLP Newsletter](#)
4. [BrainShark Video](#)
5. [Fidelity Toolkit](#)



# CYBER SAYS...

## Follow these Top Security Recommendations

Cyber and fraud best practices for protecting yourself

### Monitor Accounts and Credit

- Freeze your credit to prevent credit fraud:

**Equifax** 800-525-6285

**Experian** 888-397-3742

**TransUnion** 800-680-7289

- Monitor your accounts and credit score for suspicious activity; consider purchasing identity theft protection

### Protect Your Accounts and Identity

- Create unique login identities and passwords (avoid using your email address)
- Enable two-factor authentication for Fidelity and other financial, email, phone and social media accounts
- Provide current email address and phone number so you can be contacted in real time in case of fraud
- Sign up for voice biometrics when offered
- Don't click on untrusted links or attachments in email or text
- Consider using a password vault/manager for lower risk accounts



Phishing still drives 90% of cybersecurity breaches.<sup>1</sup> If you're in doubt,

**DON'T CLICK and DELETE!**



There are now more than **15 billion stolen** account credentials available to cybercrime actors.<sup>2</sup>

Make yourself a difficult target for cyber criminals by not reusing passwords and avoiding weak, commonly used passwords, e.g., 123456.

### Safeguard your Data, Mail and Online Shopping

- Backup your data to a secure cloud location
- Consider using trusted payment systems and never use debit cards for online purchases
- Protect your mail – sign up for USPS's free **Informed Delivery Service**

### Secure your Devices

- Use a personal firewall and anti-virus software on your personal devices
- Use trusted devices for conducting sensitive transactions
- Avoid conducting sensitive transactions over public Wi-Fi
- Secure your mobile services, including cellphone and mobile provider account
- Update/patch your Internet of Things (IoT) devices - e.g., smart TVs

1. Graphus, Inc, January 2020

2. The Digital Shadows Photon Research team as seen on Forbes.com, July 2020

# CyberWellness®

## Preventing Fraud & Identity Theft

Cyber says,

*If you connect it, protect it!*



## AGENDA



**Forces Shaping  
Cybersecurity and  
Fraud**



**Password & Account  
Protection**



**Beware of Scams**



**Secure Your Devices**



**Monitor and Freeze  
Your Credit**



**Protect Your Family**

## Forces Shaping Cyber Security & Fraud



**Proper defenses are key to preventing data breaches and fraud.**

***Ransomware** blocks company's access to data. Company pays \$1M to get data back.*

**Data breaches**

***Phishing** nabs another victim. Scam exposes employer's data to hackers.*

**Malware**



***Identity theft** leads to compromised accounts*

**ID Theft**

**Fraud**

*Hackers use **compromised credentials** to steal money out of customer accounts*





**Cybercriminals love to target accounts by using compromised login credentials.**



Check if your email or phone is in a data breach

**<https://haveibeenpwned.com>**



## Password and Account Protection



**Create Unique Login  
Identities and  
Passwords**

### Passwords

Samuel123

M0nk3y99

49lakestreet

Y#Cb3\$D6dZYF

### Pass-phrases

I LOVE ice-cream!

Jerry lives in Bugtussle KY

I can see them, y'all.

2be or not 2b, that is the ?



## Password and Account Protection



Select how you want to receive your security code

The code will be sent to  
(xxx) xxx-1234.


☐ Text Message  
Mobile phones only. Message and data rates may apply.

☐ Automated Call  
Call will come from area code 714.

[Go Back](#) [Continue](#)

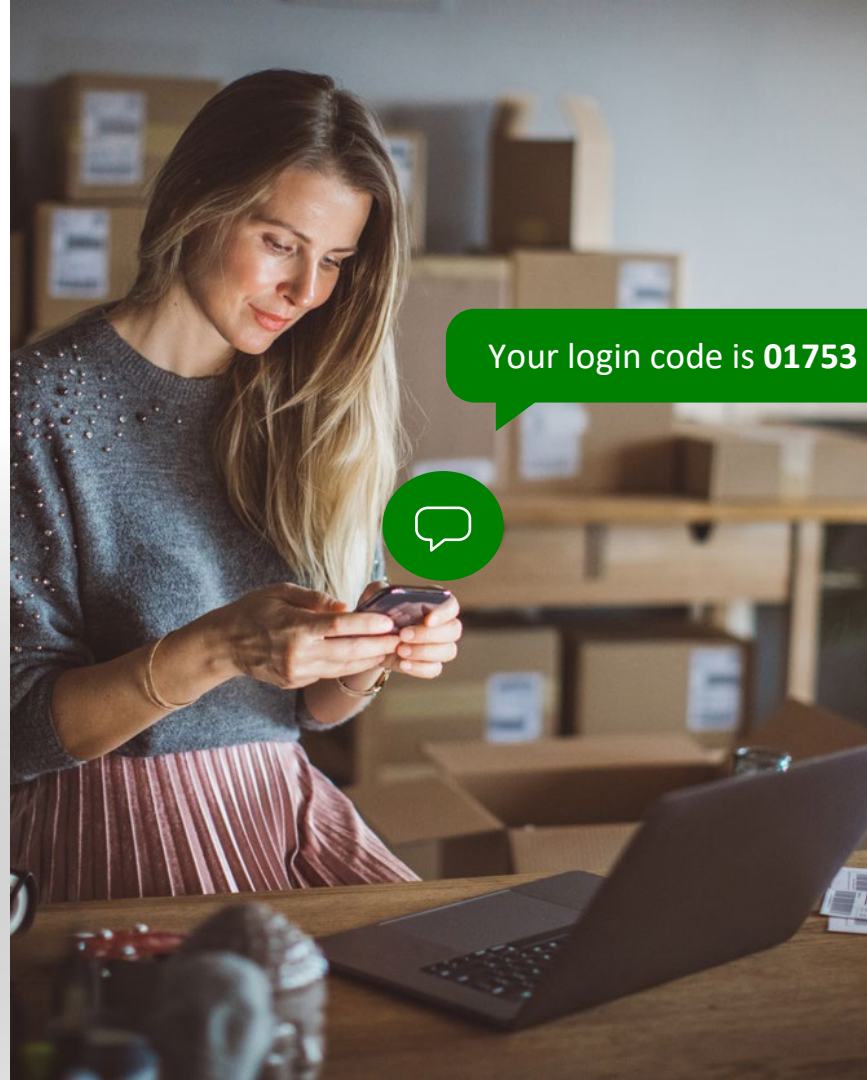
[Cancel](#)

[FAQs](#) | [Security Terms](#)



Provide your  
mobile # and email

Enable Two-Factor  
Authentication



Your login code is **01753**





Password and Account Protection



**Sign up for biometrics!**  
**“Uniquely Identifiably YOU”**

**Voice Recognition**

**Facial Recognition**



**Thumbprint**





## Smishing

Text or Instant Message

## Vishing

Phone Call

***“Nobody likes you that much.  
You haven’t won anything.  
Nothing is Free.”***





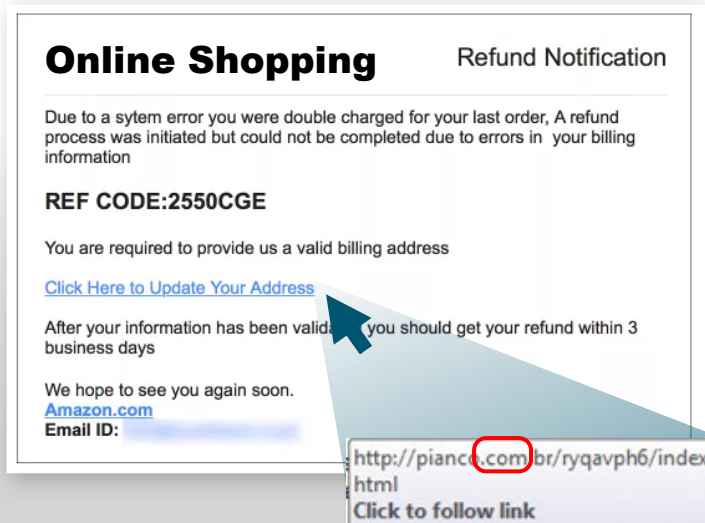
## Be Aware of Scams



**Don't Click on  
Untrusted Links or  
Attachments**

Your credit card has  
been temporarily  
suspended. To  
unlock your account,  
click here.

Congrats Kelli!  
You've been  
randomly picked for  
a \$1000 Walmart  
gift card promotion.



Last dot



http://xxxxx/amazon.com

The website owner is **always placed before the last dot** in a link

*Screenshots are for illustrative purposes.*



## Secure Your Devices



- Automatically **patch** and use a **firewall** and **anti-virus software** on your personal devices
- **Use trusted devices** for conducting sensitive transactions
- Avoid conducting sensitive activities (shopping, banking, sensitive work) over **public Wi-Fi**
- **Secure** your mobile device
- **Backup** your data to a secure cloud location

Always Patch and  
Update Your  
Devices



## Secure Your Devices



- Automatically **patch** and use a **firewall** and **anti-virus software** on your personal devices

Always Patch and  
Update Your  
Devices





## Secure Your Devices



- Automatically **patch** and use a **firewall** and **anti-virus software** on your personal devices
- **Use trusted devices** for conducting sensitive transactions







## Secure Your Devices



- Automatically **patch** and use a **firewall** and **anti-virus software** on your personal devices
- **Use trusted devices** for conducting sensitive transactions
- Avoid conducting sensitive activities (shopping, banking, sensitive work) over **public Wi-Fi**



## Secure Your Devices



- Automatically **patch** and use a **firewall** and **anti-virus software** on your personal devices
- **Use trusted devices** for conducting sensitive transactions
- Avoid conducting sensitive activities (shopping, banking, sensitive work) over **public Wi-Fi**
- **Secure** your mobile device



## Secure Your Devices

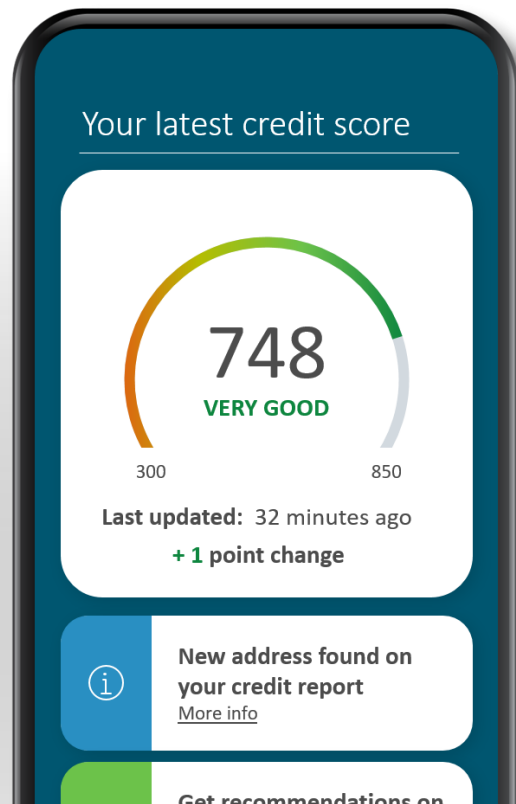


- Automatically **patch** and use a **firewall** and **anti-virus software** on your personal devices
- **Use trusted devices** for conducting sensitive transactions
- Avoid conducting sensitive activities (shopping, banking, sensitive work) over **public Wi-Fi**
- **Secure** your mobile device
- **Backup** your data to a secure cloud location





## Monitor and Freeze Your Credit



### Check for suspect activity

Profile changes  
Contact changes  
Transaction attempts  
Review alerts

You are responsible for protecting yourself

**Experian** 888-397-3742

**Transunion** 800-680-7289

**Equifax** 800-525-6285

Alerts: CreditKarma.com or Credit.com

## Protect Your Family



» **Talk About It**



» **Look for  
Warning Signs**





**NEXT STEPS**



**Be Proactive**



**Recognize the Risks**



**Secure Your Accounts**



**Secure Your Devices**

**Cyber Says.... If you connect it, protect it!**

**CyberWellness®**





NEXT STEPS



Be Proactive



## Recognize the Risks

Phishing – Email, Text, Phone  
Social Media Scams

**Cyber Says.... If you connect it, protect it!**

**CyberWellness®**





## NEXT STEPS



**Be Proactive**



### **Recognize the Risks**

**Phishing – Email, Text, Phone**  
**Social Media Scams**



### **Secure Your Accounts**

**Current Contact Information**  
**Pass *Phrases***  
**Two Factor Authentication**  
**Freeze and Monitor Your Credit**

**Cyber Says.... If you connect it, protect it!**

**CyberWellness®**



## NEXT STEPS



### Recognize the Risks

Phishing – Email, Text, Phone  
Social Media Scams



### Secure Your Accounts

Current Contact Information  
Pass *Phrases*  
Two Factor Authentication  
Freeze and Monitor Your Credit



### Secure Your Devices

Screen Lock  
Voice, Fingerprint, Facial Recognition  
Automatic Updates  
Caution with Public Wi-Fi  
Data Backup

Be Proactive

**Cyber Says.... If you connect it, protect it!**

**CyberWellness®**

## Additional Resources



Fidelity's [Personal Security Checklist](#)

[5 Ways to Protect Yourself from Cyber Fraud](#)

---

FTC guidance to help you avoid fraud from [common online scams](#)

[Securing Wireless Networks](#)

---

If you're a victim of online crime, file a complaint with the [Internet Crime Complaint Center](#), or visit the FTC's free, one-stop resource, [www.IdentityTheft.gov](http://www.IdentityTheft.gov)

---

# Important Information

Third-party trademarks and service marks are the property of their respective owners. All other trademarks and service marks are the property of Fidelity Management & Research LLC or an affiliate.

Experian and Fidelity Investments are independent entities and are not legally affiliated.

Transunion and Fidelity Investments are independent entities and are not legally affiliated.

Equifax and Fidelity Investments are independent entities and are not legally affiliated.

Approved for use in Advisor and 401(k) markets. Firm review may apply.

©2022 FMR LLC. All rights reserved.

Fidelity Brokerage Services LLC, Member NYSE, SIPC, 900 Salem Street, Smithfield, RI 02917

981854.3.0