PRESENTED BY: DAVID SCHNEIER – FIDELITY CUSTOMER PROTECTION

Protecting what matters:

Our customers' trust and financial future

Fidelity INVESTMENTS

DOL Issues Guidance on Cybersecurity, April 2021

Three focus areas for plan sponsors, recordkeepers, and participants

Plan sponsors

Designed to assist plan sponsors fiduciaries in their evaluation of the cybersecurity practices of service providers.

View guidance

Cybersecurity Best Practices

Best practices for recordkeepers and other service providers outlining key elements of a cybersecurity program.

View guidance

Online Security Tips for Retirement Investors

A series of recommendations for plan participants to prevent fraud and loss of access to a retirement account.

View guidance

When participants are victims of fraud, plan sponsors may be responsible

Fraud

Recordkeeper, Plan Sponsor Charged in 401(k) Account Theft

Alleged fraud drains retiree's 401(k)

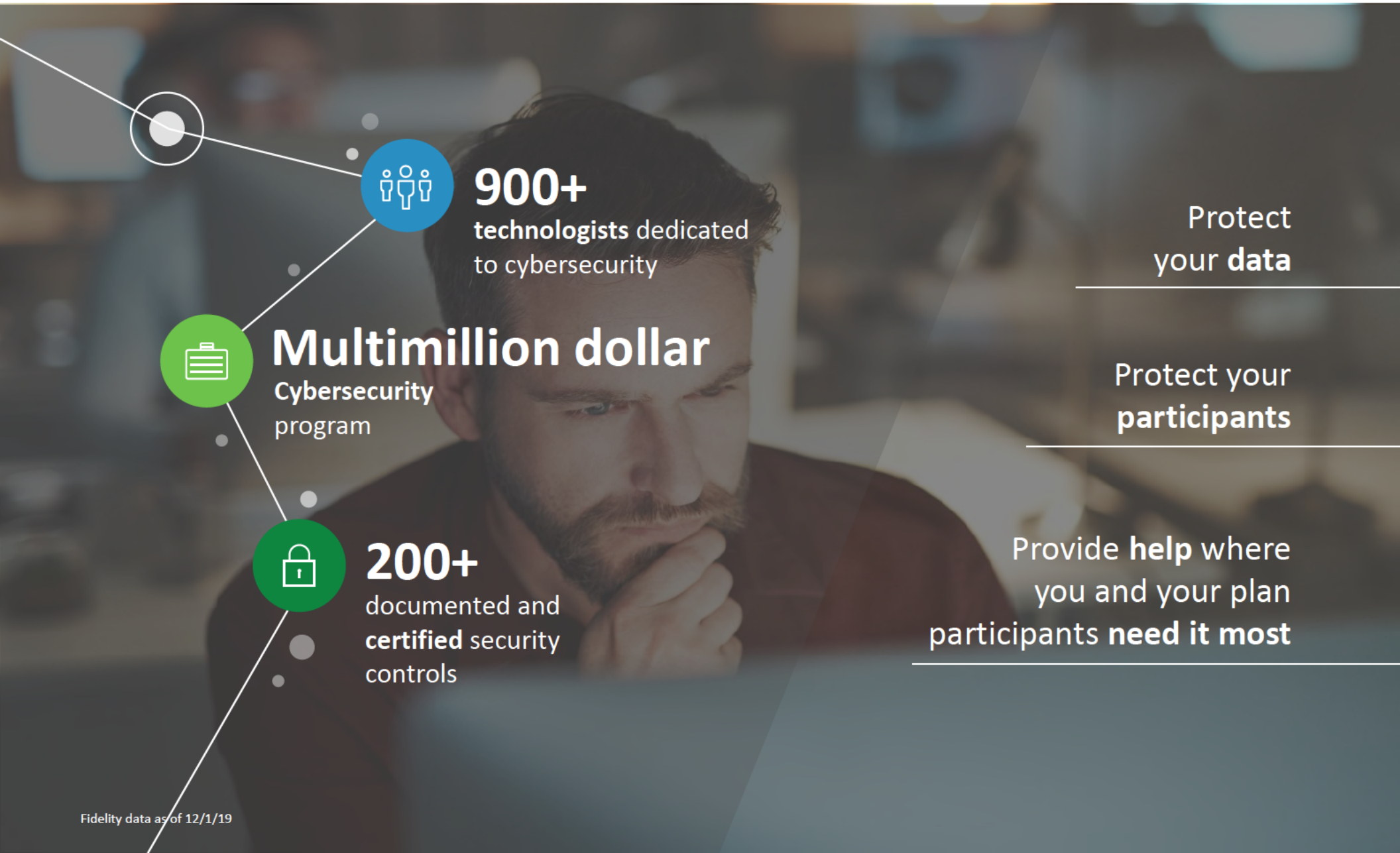
Plan's administrator facing federal probe into unauthorized distributions

Lawmakers Ask GAO to Examine Cybersecurity of Retirement System

What are you doing to ensure the security of your employees' accounts?

Fidelity is committed to protecting our customers

We keep your data and employees safe with significant investments in cybersecurity



We protect and treat your data as if it were ours

Comprehensive controls, processes, and systems in place to help ensure your data is safe, secure, and private

We employ National Institute of Standards and Technology (NIST) Cybersecurity Framework

Guidelines to **create**, **guide**, **assess,** or **improve** comprehensive cybersecurity programs

Industry certifications

ISO 27001

International gold standard for information security

- **Certified since 2011**
- **Must pass over 114 unique security controls**

ISO 27701

NEW! Data privacy

ISO 22301

Business resiliency program

We protect your greatest asset: your employees

An industry-leading[1] customer protection program focusing on protecting individual customers from account compromise, fraud, and identity theft

Proprietary fraud detection and prevention

Anomalous activity and pattern recognition utilizing internal and external intelligence

Compromised credential testing

In the last 4 years, **1,200,000+ Fidelity accounts have been proactively blocked[2]**

Account protection features

Two-factor authentication

Real-time alerts for high-risk transactions

MyVoice® phone authentication

50% of calls are authenticated with MyVoice[2]

Click to view demo

Fidelity's Customer Protection Guarantee

Participants reimbursed for losses from unauthorized activity through no fault of their own, with no dollar limit

Click to view guarantee

[1]Fidelity ranked No. 1 in customer security out of seven leading brokerage firms in the 2018 User Authentication and Security Practices study conducted by Corporate Insight.
[2]Fidelity Investments data as of 3/31/20

DOL's guidance on cybersecurity 12 best practices

Using industry guidance to help protect your firm

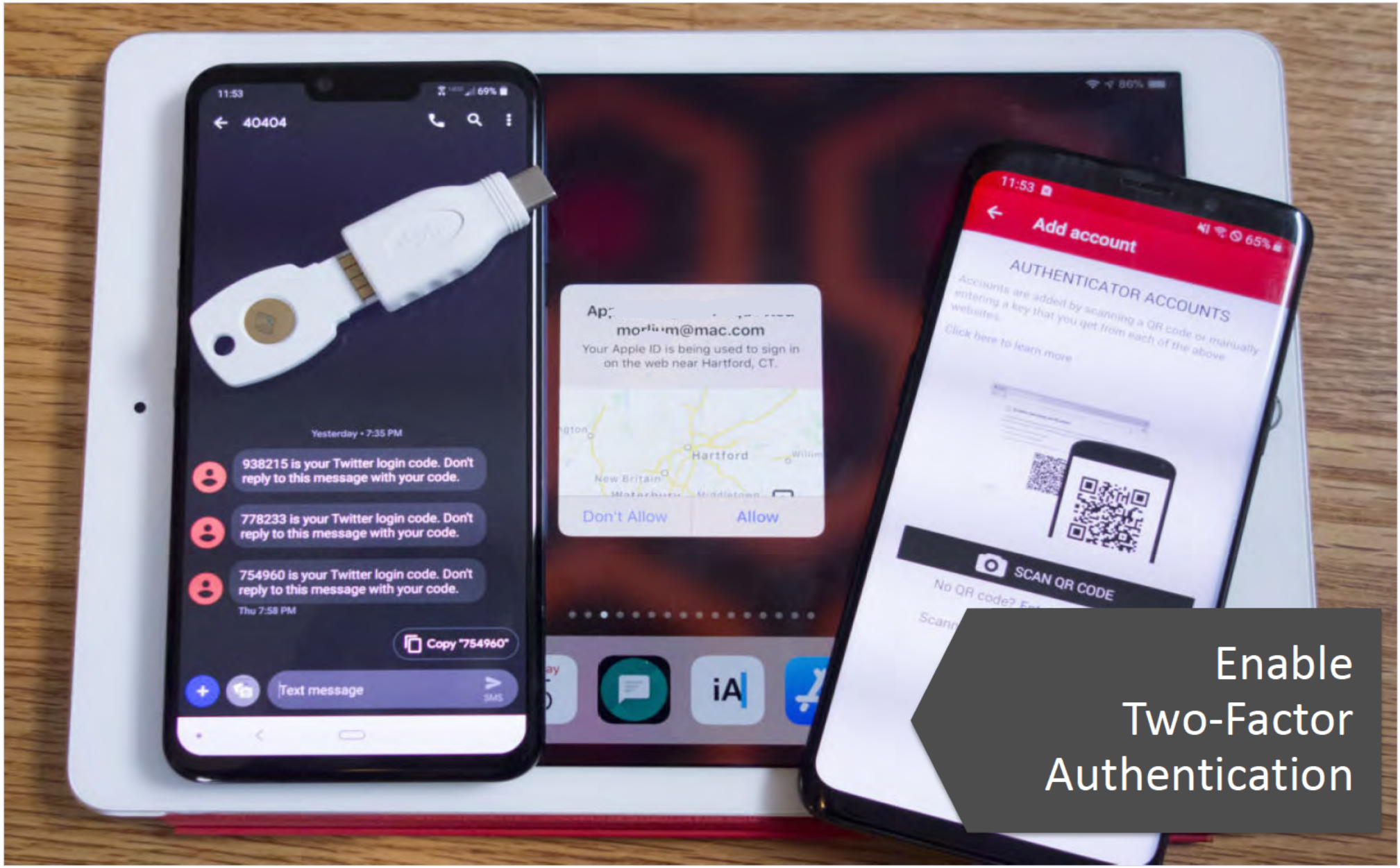
1. **Have a formal, well documented cybersecurity program.**
2. **Conduct prudent annual risk assessments.**
3. **Have a reliable annual third-party audit of security controls.**
4. **Clearly define and assign information security roles and responsibilities.**
5. **Have strong access control procedures.**
6. **Ensure that anywhere sensitive data is stored is subject to appropriate security reviews and independent security assessments.**

DOL's guidance on cybersecurity 12 best practices

Using industry guidance to help protect your firm

7. **Conduct periodic cybersecurity awareness training.**
8. **Implement and manage a secure system development life cycle (SDLC) program.**
9. **Have an effective business resiliency program addressing business continuity, disaster recovery, and incident response.**
10. **Encrypt sensitive data, stored and in transit.**
11. **Implement strong technical controls in accordance with best security practices.**
12. **Appropriately respond to any past cybersecurity incidents..**

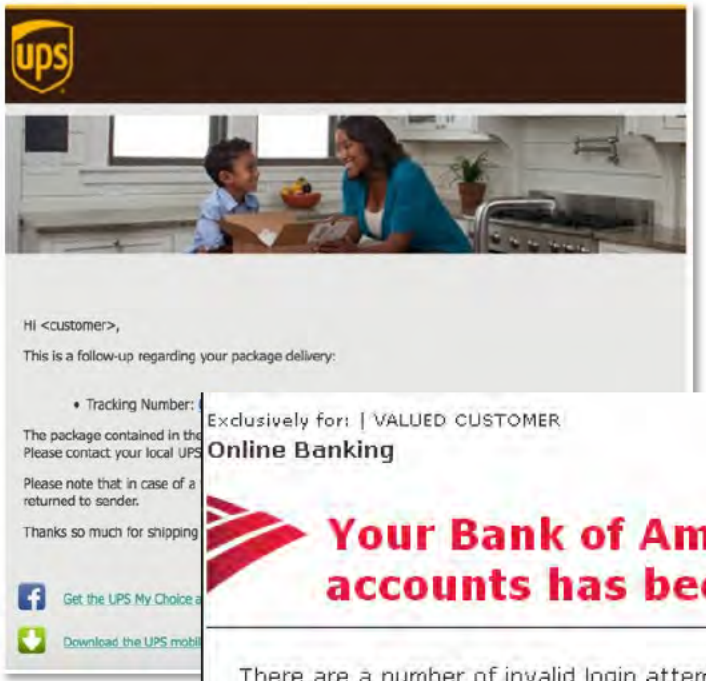

Password:
Create unique passwords

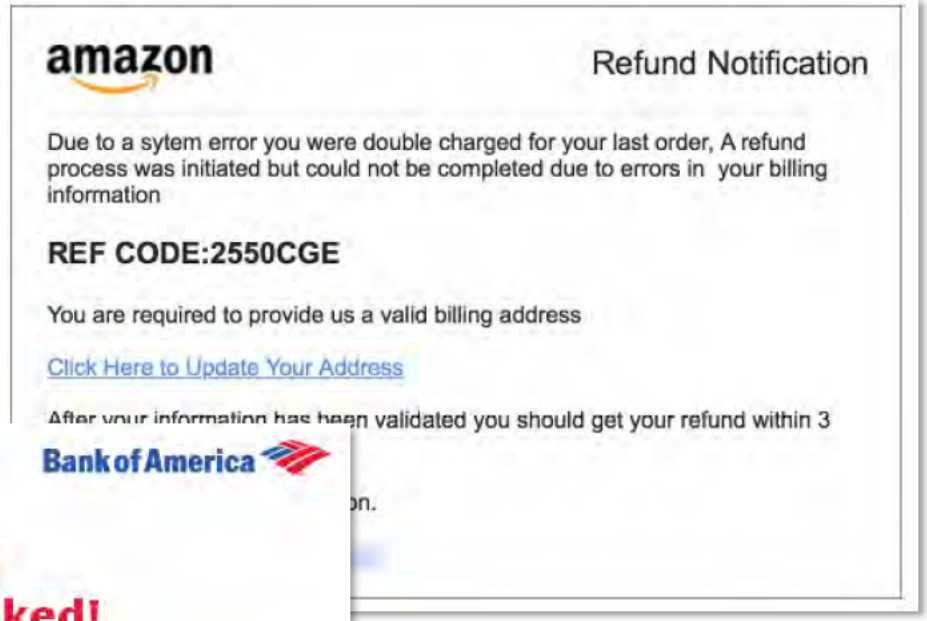


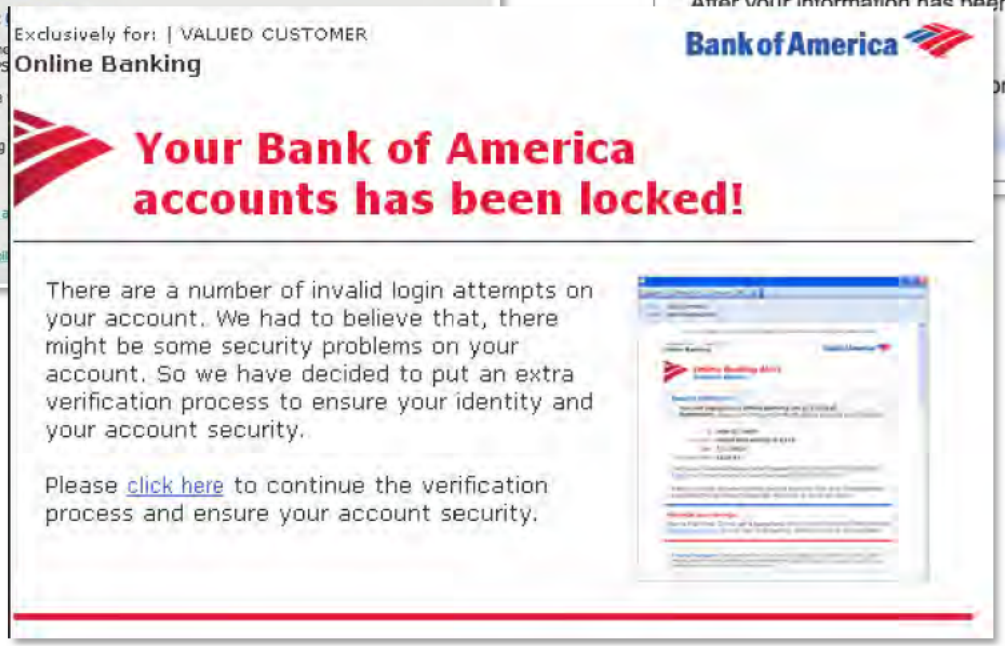
Fidelity INVESTMENTS

Secure Your Cell Phone Account

Fidelity INVESTMENTS



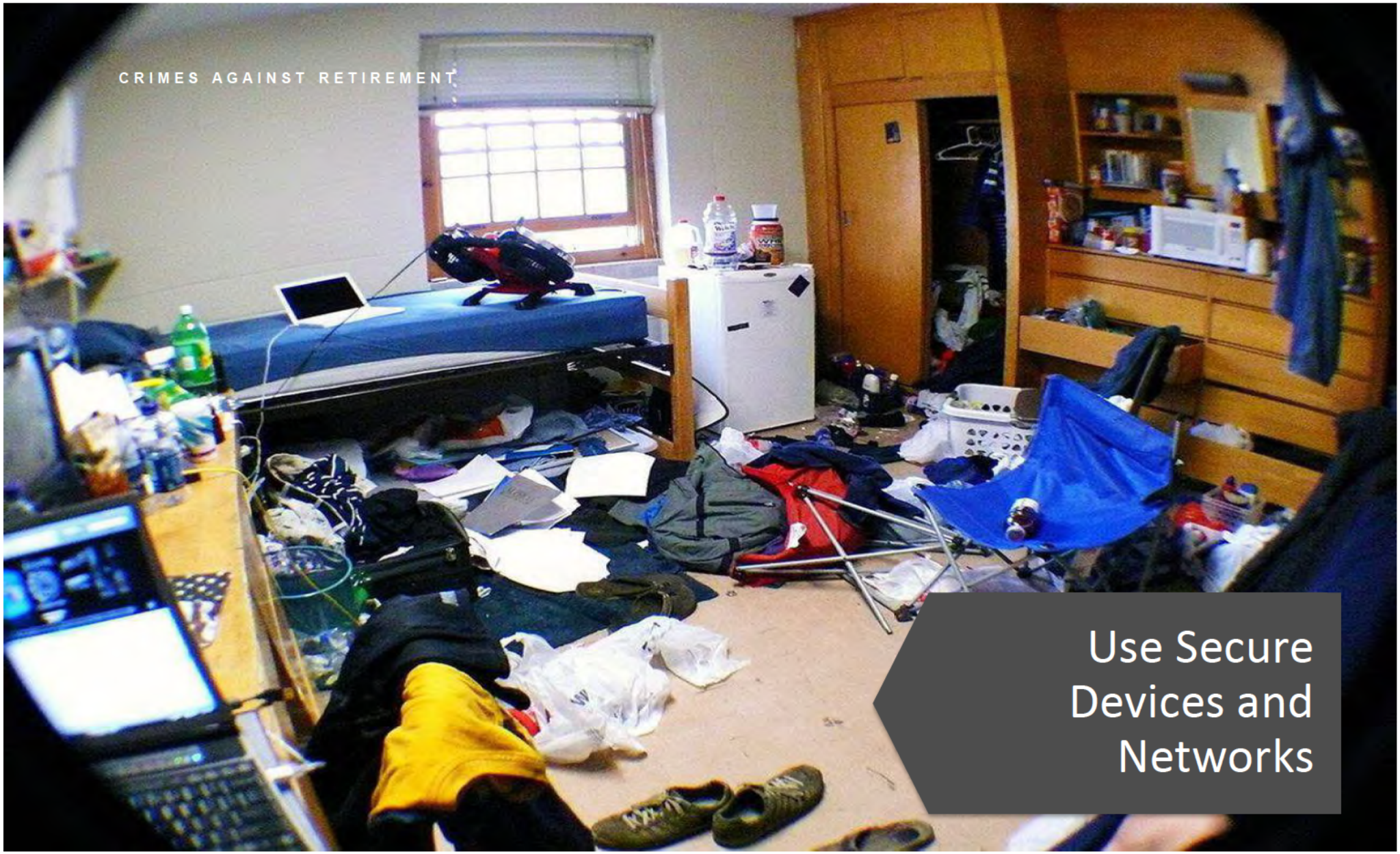




Don't Click On A Phish

Fidelity INVESTMENTS


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specifi
After your payment, click <Check Payment>. Best
Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00
Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $600 worth of bi
13AM4VW2dhxYgXeQe
Check Payment
Decrypt
Backup Your Data



Use Secure Devices and Networks

Fidelity INVESTMENTS


Update your devices

Fidelity INVESTMENTS

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.[1] If you're in doubt,

DON'T CLICK and DELETE!

There are now more than **15 billion stolen** account credentials available to cybercrime actors.[2]

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

Fidelity INVESTMENTS