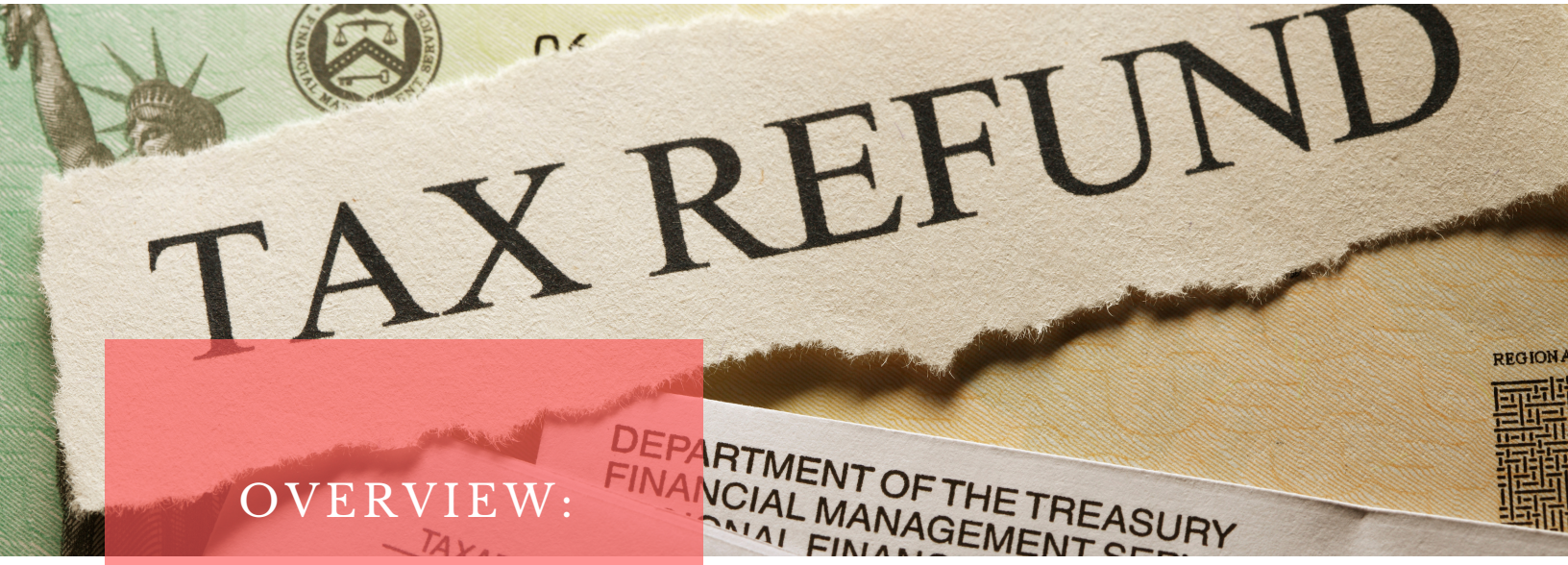
VOLUME 2 | ISSUE 4

THE TECHNOLOGY BYTE

NEWSLETTER FROM YOUR TECHNOLOGY GUIDE:
ACE TECHNOLOGY GROUP



OVERVIEW:

TAX SCAMS

Tax Deadline Monday, Apri 18, 2022

Tax day is getting closer and criminals prey on stress and fear. Many taxpaying citizens fear the IRS and will do just about anything to pay the taxes they think they owe.
The perfect recipe for scammers to steal your social security number or your tax refund.

Three common tax-related scams:

- **Tax-Related ID Theft** - this happens when scammers steal your personal ID - including SSN, birthdate, address, and use it to file a tax return in your name. Criminals do this so they can steal your tax refund.
- **The Gift Card Scam** - Scammers use this all-to-common tax scam by scaring taxpayers into believing they are in danger of being charged with criminal activity and that the penalty fee is paid with gift cards.
- **Refund Recalculation Scam** - Criminals send an email or text telling taxpayers they're getting a bigger refund. Those notifications include a phishing link that requires personal identification - SSN, birthdate, etc. Once that info is entered the criminal steals your ID.

Odds are if you get a call or email from the IRS it's a scam. The IRS does NOT reach out through email, phone calls, or texts. And NEVER asks for personal information.

ACE Technology Group

RECENT SECURITY BREACHES IN THE U.S.

Microsoft
Exploit: Unauthorized Access

Morgan Stanley
Exploit: Social Engineering (Vishing)

H.P. Hood Dairy
Exploit: Hacking

UNDER THE HOOD

VoIP Phone Safety

To protect our phone customers from VoIP-related attacks, we only allow the phones to communicate with the phone server directly and only allow the phone server to communicate with the phones from certain IP addresses.

Attackers are able to mimic an extension and make calls from their account, potentially costing the business money. They are also able to repeatedly call the business's phone system and prevent important calls from coming in.

It's important to take phone safety seriously, especially since it's easy to fall victim to social engineering calls that trick people in giving away important financial information. One of these phone scams includes receiving a call from someone saying they're from Microsoft and that they need to connect into a company or personal computer to resolve an issue, cleanup a virus, etc. The caller ends up asking for credit card information and charging a lot of money for these services.

What is Business Email Compromise (BEC)?

CHRIS'S CORNER

Monthly Expert Advice From The Owner

"Business Email Compromise (BEC) is an exploit in which an attacker obtains access to a business email account and imitates the owner's identity to defraud the company and its employees, customers, or partners."

Cybercriminals often create an email address almost identical to the owner or CEO. The scammer hopes that it is a trusted email address, and minor differences in the email account will go unnoticed by the victim. Hackers focus their efforts on the employees with access to company finances. They attempt to trick these employees into carrying-out wire transfers to unsecured bank accounts, where the money ends up in criminals' hands.

If the money fraud fails to be spotted in a timely manner, the funds can often be close to impossible to recover, due to any number of laundering techniques that transfer the funds into other accounts.

Techniques for Business Email Compromise

- Spoofing email accounts and websites: Slight variations on legitimate addresses (jane.doe@abccompany.com vs. jane.doe@abc.company.com) fool victims into thinking fake accounts are authentic.
- Spear-phishing: Bogus emails believed to be from a trusted sender prompt victims to reveal confidential information to the BEC perpetrators.
- Malware: Used to crack networks in order to gain access to internal data and systems. A tactic used to view reliable emails regarding the finances of the company. That information is then used to avoid raising the suspicions of any financial officer when a falsified wire transfer is submitted. Malware also lets criminals gain access to their victim's sensitive data.

Cybercriminals target businesses big and small. Cyber security is more essential now than ever before. A compromised email account can seriously damage businesses, causing some to close their doors permanently. Protecting your company's finances and privacy will not only empower your employees but also ensure your business tenure.

LATEST IN CYBER SECURITY

FBI Internet Crime Report for 2021 - $6.2 Billion Lost to Cyber Crimes

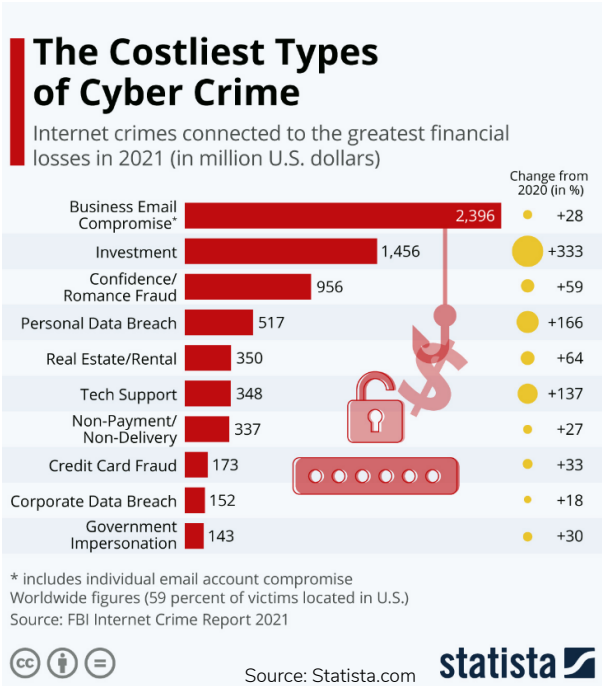
The FBI recently released their Internet Crime Report for 2021. The report contains losses collected from around the world, but many of the losses reported were in the United States. In 2020 the estimated loss was $4.2 billion. The FBI's latest report shows the estimated loss for 2021 has increased to $6.2 billion.

Out of the overall statistics, Pennsylvania ranked #8 with 17,262 victim complaints and #5 with a total loss of $206,982,032. New Jersey ranked #10 with 12,817 victims and a loss of $203,510,341. The United States ranked #1 (59%) in the number of victims impacted according to the report.

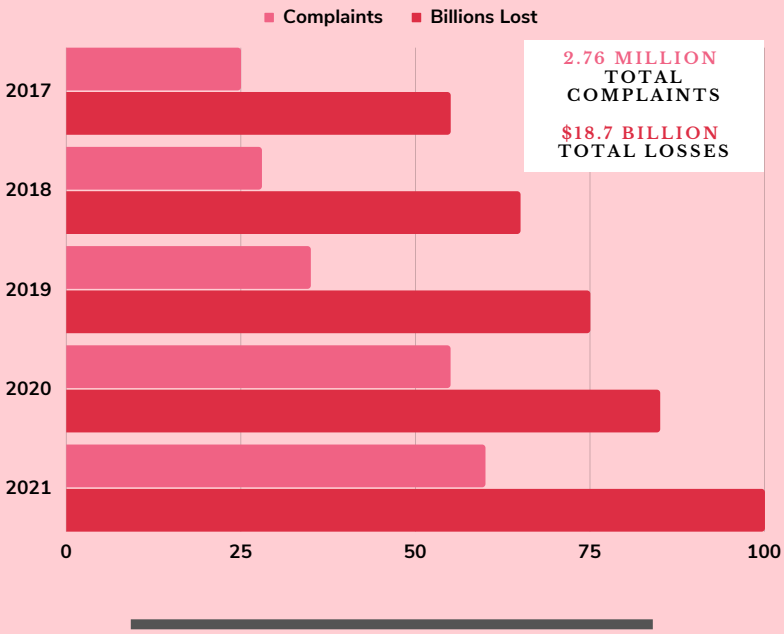
Adults 60 and over filed 92,371 victim complaints resulting in a loss of $1.68 billion. Ages 50-59 had 74,460 complaints resulting in a loss of $1.26 billion, while adults 40-49 had 89,184 victims that lost $1.19 billion. Victims under the age of 20 were 14,919 resulting in a loss of $101.4 million.

The costliest internet crime reported by the FBI was business email compromise (BEC) and personal email compromise. Cybercriminals target businesses and individuals by sending fraudulent emails. Many times this results in the victim engaging in wire transfers. In 2021 almost $2.4 billion was lost due to compromised emails.

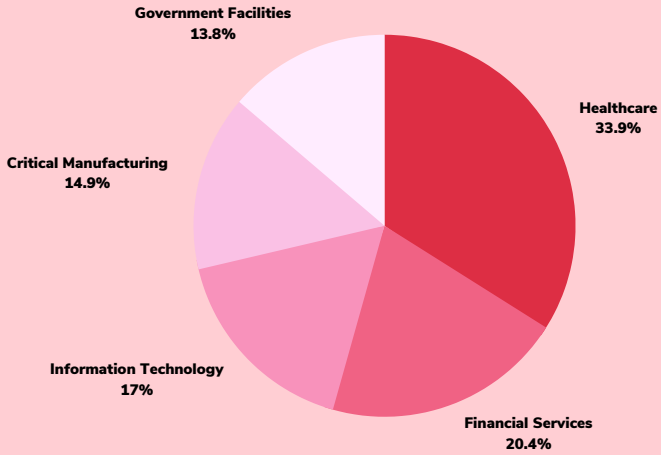
The second top costliest internet crime was investment scams with a loss of almost $1.5 billion. Losses from romance scams, personal data breaches, and real estate scams also increased, with a loss reported of just under $3 million. Tech support scams reported a loss of just under half a million.



Complaints and Losses Over 5 Years



Ransomware Attacks by Infrastructure



649 Infrastructure Ransomware Complaints Reported in 2021 by the FBI

CYBERSECURITY TERMS TO KNOW

BAD RABBIT

A strain of ransomware: Disguised as an Adobe Flash installer, a Bad Rabbit attack spreads through drive-by downloads on compromised websites, meaning victims could be exposed to the virus simply by visiting a malicious or compromised website. The Bad Rabbit malware is embedded into websites using JavaScript injected into the site's HTML code.

REMINDER

REMINDER TO FILL OUT OUR CUSTOMER SURVEYS AFTER A TICKET IS CLOSED. YOUR FEEDBACK HELPS MAKE OUR CUSTOMER SERVICE EVEN BETTER!

NEW IN TECHNOLOGY

Looking into the Future of Smart Contact Lenses

Source CNET

While not approved for everyday use, Mojo Vision's Mojo Lens is a prototype of smart contact lenses and another step closer to reality. The Mojo Lens is a self-contained, display-enabled lens that, in a sense, is augmented reality (AR).

Designed to function like a smartwatch, these hard lenses have a monochrome green display that can show basic graphics, text, and some illustrations. Fun fact, they also include eye-tracking.

While virtual reality (VR) and AR glasses use cameras to sense eye movement, the Mojo Lens follows your eye movements by sitting directly on your eyes. Similar to a smartwatch, the Mojo Lens can calculate movement more accurately than AR or VR glasses.

The lens is designed to sit on the pupil, where a display window will line up with the fovea, the center of our vision, making a ring-like circle that hovers over an app icon and then opens it up.

Imagine glancing around the room and seeing pieces of information pop up in bright displays of etched light, hanging in the air, and then disappear right in front of you. App-like widgets would display readable texts like a teleprompter. A widget popup could show your fitness goals, heart-rate and more.

The Mojo Lens is just a prototype and must be approved by the FDA before it's made available to the public. The company also needs to work on making the lenses seem more natural-looking. Not everyone wants to walk around with a bionic-looking eyeball. Read the full story.

Get to know your friendly ACE team!

EMPLOYEE SPOTLIGHT: CHRISTIAN

Service Desk Manager, West Chester native, 12+ years of experience and 1000+ accredited hours with certifications in HIPAA Security and Privacy

Known for his ability to defuse a situation and turn a negative into a positive, Christian is best at solving VoIP phone issues. A product that Christian has seen evolve and accommodate customers is Cloud Hosting, as it allows users and businesses to work from anywhere, anytime.

On Sundays and when Christian isn't working, he enjoys watching/playing hockey, practicing the upright bass or mandolin. His favorite nonprofit is the Salvation Army because of their commitment to the community and because 96% of the proceeds go directly to helping people.

- Excited about helping people
- Passionate about upright bass, the mandolin, and restaurants
- Won't give up music
- Wants to be remembered as someone who left the earth a better place than when he came into it

POWER COMMANDS

Save the Current Document

For Windows: Ctrl + S

For Mac: Command + S

Open a New Tab or Window

For Windows: Ctrl + N

For Mac: Command + T

Find us on LinkedIn