MAY 2026 | MONEY NOTES

Today's fast-moving digital landscape has transformed the way we interact with the world, including the way we bank, invest, and manage wealth. Online access, mobile apps, and automated transfers have made financial management faster and more convenient than ever before. But those same tools come with a word of caution.

Financial cybersecurity – the practice of protecting your financial accounts, personal data, and digital identity from online threats – is very much on the BLBB radar.

What Is Financial Cybersecurity?

Financial cybersecurity refers to the practices, tools, and behaviors used to protect financial accounts, personal data, and digital financial records from unauthorized access, theft, and fraud. Understanding cybersecurity is a critical part of sound financial planning.

The Most Common Types of Financial Cybercrime

The most prevalent forms of financial cybercrime share a common goal: gaining unauthorized access to your money or personal information.

> Cybercrime costs the global economy about $445 billion every year[1]

Phishing and Spoofing Scams

Phishing scams are one of the most widespread forms of digital fraud. Phishing is a type of cybersecurity attack that impersonates someone else in an attempt to secure confidential information such as passwords or account numbers. Common phishing attack examples include:

- Fraudulent emails that appear to come from your bank or other trusted sources complete with realistic logos
- Messages expressing a sense of urgency warning of suspicious activity or asking you to verify account information
- Spoofed emails or phone numbers that falsify the sender's identity to look like a legitimate source[2]

Social Engineering and Impersonation

Social engineering scams rely on human psychology. Fraudsters may call you directly on the phone, posing as customer service representatives, financial advisors, government officials, or even family members.

Malware and Digital Theft

Malware is malicious software secretly installed on your device, often through a suspicious link or email attachment – it can silently capture keystrokes, access screenshots of financial portals, or transmit login credentials to remote servers.

Business Email Compromise

Business email compromise (BEC) is a sophisticated scam in which cybercriminals impersonate a trusted contact – often an executive, attorney, or financial professional – and request an urgent wire transfer or account change. These attacks are carefully researched to appear completely legitimate.

How Does Identity Theft and Account Takeovers Happen?

Digital identity theft occurs when criminals obtain enough personal information to access your financial accounts, apply for credit in your name, or assume your identity for fraudulent purposes.

Warning signs of account takeover include:

- Unexpected password reset emails
- Login alerts from unfamiliar locations or devices
- Unrecognized transactions or changes to account settings
- Being locked out of accounts without explanation
- Missing financial statements or bills (a sign your mailing address was changed)
- Credit inquiries for new accounts you did not open

Even if you practice good personal security hygiene, a breach at a company that stores your data – a credit card company, insurance provider, or financial planning platform – can expose your information without any action on your part.

How AI Is Creating New Financial Cybersecurity Risks

Artificial intelligence has brought tremendous benefits to financial services – but it has also given cybercriminals powerful new tools.

Key AI-driven threats include:

- AI-generated phishing emails are now nearly indistinguishable from legitimate communications. Where earlier phishing attempts were often riddled with errors, AI tools can generate highly convincing, personalized messages at scale.
- Deepfake fraud uses AI-generated voice or video to impersonate financial advisors, executives, or even family members, convincing victims to authorize transfers or share credentials
- Automated account scanning tools that probe financial platforms for weak passwords or security gaps at scale
- AI-powered social engineering scripts tailored to individual psychological profiles scraped from social media

According to IBM's 2024 Cost of a Data Breach Report, 16% of all breaches now involve AI-driven attacks, including phishing and deepfake impersonation – a figure that continues to rise as AI tools become more accessible.[3]

How is BLBB Protecting Your Financial Data?

- We use **multi-factor authentication** on our client portal, **encrypted document delivery**, and strict **role-based access controls**.
- Third-party vendors and technology partners who access client data must maintain appropriate **security standards and data protection practices**.
- Any large money movement submitted via E-mail is **verified by phone** before processing – as are transfers to new or previously unrecognized destinations, requests originating from a third party on a client's behalf, and any inbound communication that raises a concern about fraud or impersonation.
- Participate in **regular cybersecurity training** in adherence to our formal **Written Information Security Policy** in accordance with SEC requirements.

At BLBB, protecting client data and assets requires layers of security – not a single lock on the door.

Best Financial Cybersecurity Practices

These cybersecurity best practices significantly reduce your exposure to digital fraud and identity theft:

- Enable **multi-factor authentication (MFA)** which adds a second layer of verification that makes it significantly harder for criminals to gain access even if they have your password.
- Use **unique, strong passwords** and a password manager to generate and store complex passwords securely.
- **Verify wire instructions independently** by calling the recipient directly using a phone number you have independently verified – not one provided in the wire instruction email.
- **Monitor account activity regularly** and set up transaction alerts where available.
- **Avoid accessing financial accounts on public Wi-Fi** networks that are frequently unsecured and susceptible to interception.
- **Keep devices and software updated** against known vulnerabilities that cybercriminals actively exploit.
- **Review financial statements monthly** for unusual activity, unfamiliar charges, or unauthorized account changes – even small transactions, which criminals sometimes use to test accounts before larger withdrawals.

What to Do If You Become a Victim of Financial Fraud[4]

If you suspect you have been the target of financial fraud, digital identity theft, or account takeover, *acting quickly* can help limit the damage.

- Contact your financial institution(s) and wealth advisor immediately.
- Change passwords and secure all accounts.
- Document all suspicious communications.
- Freeze your credit if personal information is compromised.
- Report the crime[5] to the appropriate authorities.

Financial Cybersecurity FAQs

What is financial cybersecurity?

Protection of financial accounts, personal data, and digital financial activity from cybercrime, fraud, and identity theft

What are the most common financial cybersecurity threats?

- phishing scams
- digital identity theft
- wire fraud
- investment fraud
- malware attacks

How can I prevent digital fraud?

Enabling multi-factor authentication, using strong and unique passwords, verifying financial requests before acting on them, monitoring accounts regularly, and staying informed about emerging fraud tactics is equally important

What should I do if my identity is stolen?

Act immediately - contact your financial institutions, change passwords, document all suspicious activity, freeze your credit, and report the theft through official resources

---

[1] https://www.sbir.gov/tutorials/cyber-security/tutorial-1
[2] https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing
[3] https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
[4] https://consumer.ftc.gov/articles/what-know-about-identity-theft
[5] https://www.ic3.gov

L to R: Robb Parlanti, Laura LaRosa, Clif Haugen, John Lawton, Laura Brewer, Dean Karrash, Brian Gallagher, Brianna March, Nick Bucci, Bob Flood, Mike Geraghty, Zack Renna