Staying safe online: Simple steps to avoid cyberattacks

Online cybercrimes of various types are on the rise across a broad range of industries—including higher education, healthcare and finance. Accessing and monetizing sensitive data is often the goal—and it's working.

Consider taking these simple steps to protect your sensitive data:

1. **Use multifactor authentication (MFA)** everywhere it is available. Using multiple factors to authenticate into an account makes it much more difficult for hackers to access your accounts.
2. **Use a different password** for every site and create complex passphrases with 12 or more characters. **A 12-character password takes 62 trillion times longer to crack than a 6 character password.**[3]
3. **Be wary of oversharing** information online. Fraudsters use overshared data on social media channels for social engineering attacks.
4. **Be vigilant in spotting phishing attacks**. These ploys aim to trick you into sharing your passwords, account numbers or other sensitive information. If that happens, fraudsters may be able to access and control your accounts.
5. **Keep personal contact information current** so you can be reached if an attack occurs.
6. **Regularly monitor your credit score** and online accounts. Close and delete unused accounts.
7. **Use antivirus software** and update software, hardware, and applications. Updates include security upgrades to keep your devices safe.
8. **Know how to report identity theft** and cybersecurity incidents.
   - If you are the victim of online or internet-enabled crime, file a report with the **Internet Crime Complaint Center (IC3)**.
   - If you or your organization is the victim of a network intrusion, data breach, or ransomware attack, contact your **nearest FBI field office** or report it at **tips.fbi.gov**.
   - Phishing and identity theft concerns can be reported through the CISA, FTA, and SSA **here**.
   - For TIAA, report a suspicious email at **abuse@tiaa.org** or by calling **800-842-2252**.

44%

of security teams say they've lost confidential data in 2022 due to a data breach—up from 28% one year ago.[1]

99%

of account compromise attacks can be blocked using MFA.[2]

At TIAA, customer data security is a responsibility and a top priority. We combine technology, people, and processes to meet that responsibility and we comply with both state and federal laws, regulations, and industry guidelines. For more information, please visit the **TIAA Security Center**.

[1] Splunk: **The State of Security 2022**.

[2] Microsoft: **One simple action you can take to prevent 99.9 percent of attacks on your accounts**, August 2019.

[3] Scientific American: **The Mathematics of (Hacking) passwords**, April 2019.

2444376
P0355214

(10/22)