It’s Up to Us

Simple Steps for Cyber Safety

By Justin Macksamie, Senior Cybersecurity & Information Security Analyst

September 28, 2022

I’m not one for scare tactics or fearmongering, but here’s the cold, hard truth: no one is immune to cybercrime. Not you, not me, not the world’s largest companies nor the smallest – no one. Data breaches that include usernames, passwords, emails and even credit card information happen all the time. In September alone, Uber, The North Face and Samsung all experienced data breaches that exposed their customers’ data. In 2021, cybercrime cost businesses nearly $7 billion in losses, a majority of which stemmed from email compromise, such as phishing. Phishing attacks are the most common vector for attackers to gain a foothold in an organization. Phishing is also commonly used against everyday people to steal their bank account or credit card information, or to trick them into making illegitimate payments.

The Crossroads of Cybersecurity & Fraud Prevention

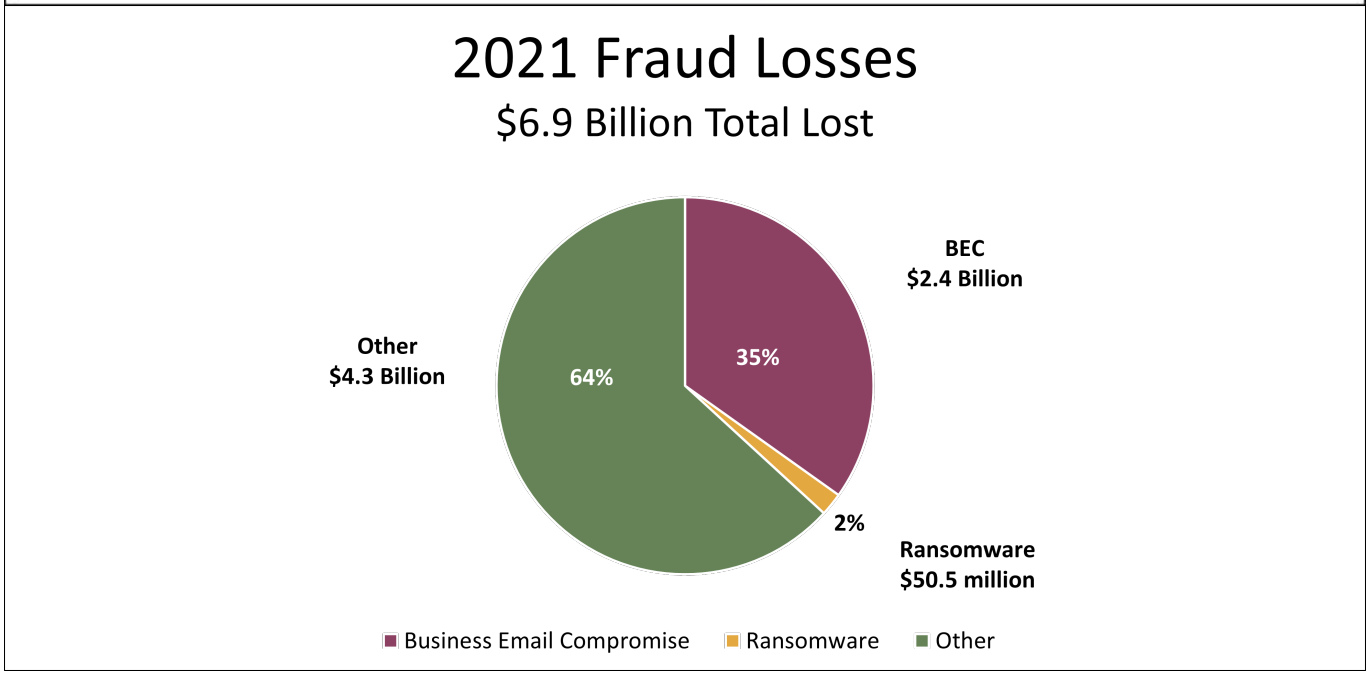
Presented by Dean Choudhri
and Neil Kumar
Recorded 11/8/2022

View webinar and download presentation slides

Since 2004, October has been commemorated as Cybersecurity Awareness Month. In its nineteenth year, the awareness campaign theme is “See Yourself in Cyber,” to remind us that while cybersecurity may seem like a complex subject, it all boils down to people. People like you, people like me, who have careers, families, responsibilities and hobbies. No matter who you are or what you do, it’s crucial we all take basic steps to protect our online data and privacy, both at work and at home.

1. Be suspicious of emails, texts and phone calls from unknown senders.

- Phishing is not only the most common method for attackers to breach corporations, but also normal people in everyday life. Common scams include IRS payments, Amazon account issues, package tracking numbers, fake virus alerts, phony tech support, and current events that can be monetized (e.g., hurricane relief).
- If something seems suspicious, do not respond to the message. Report it and delete it.
- Many organizations have a fraud-reporting email address where you can send suspicious emails or text message for further investigation.



2. Use strong and unique passwords.

- Don’t repurpose your passwords between different websites or services. If your online bank account uses the same credentials as your Uber account, your bank account is now highly vulnerable to hacking!

- Using pass phrases is an easy way to increase password complexity while keeping it easy to remember. OctoberIsCybersecurityAwarenessMonth2022! has 41 characters, including upper and lowercase letters, numbers and special symbols. It would take over 100 years for a hacker to break that password.

3. Use multi-factor authentication (MFA).

- MFA adds another layer of security to your online accounts. Even after a successful login, you must provide additional information, such as a text message code or a push notification. So even if an attacker has your login credentials, they will not be able to access your account without your MFA authorization.
- If you receive an unsolicited MFA alert, this might be an indication that your credentials have been leaked or compromised.

4. Be cautious of public wireless internet.

- Open WiFi networks can be dangerous because you don't know who might be "eavesdropping." Hackers can collect transferred information through an open wireless network.
- If you use an open wireless network, make sure any site you access uses HTTPS. This will block an attacker on the network from reading any data that you transmit to the website.
- For an extra layer of security, use a Virtual Private Network (VPN). A VPN creates a private tunnel that no one else on the network can access.

5. Monitor your credit card and banking statements.

- The unfortunate reality is that many companies have been breached, with millions of records stolen. Be sure to regularly check for unusual activity.
- Consider setting transaction alerts. Many banking companies allow for alerts when purchases are made or money is transferred.

It's time we see ourselves as key pieces of the cybersecurity puzzle. For additional cybersecurity tips and information, feel free to contact Alloya's Cybersecurity & Information Assurance Department at **cybersecurity@alloyacorp.org**.