Munching On Mobile Cybersecurity Tips

cyber security technology mobile risk

Summary: Mobile apps - including banking apps - are more at risk now than ever before. A Verizon report provides details on the types of risks and the practices recommended to protect your bank.

We aren't dieticians, but found it certainly interesting that research finds you burn more calories eating celery than it contains. After all, it only has 6 calories and is about 95% water. The good news is that one cup of celery gives you about 30% of the recommended daily intake of Vitamin K, which plays a key role in helping blood to clot and assisting in absorption of calcium from food. Of note, celery is part of the parsley family, which also includes carrots and cumin.

While certainly not as good for you as the crunch of a good stalk of celery, bankers are also getting crunched by mobile security cyber incidents.

To get a better view on steps security professionals are taking to mitigate mobile threats, we looked at a survey by Verizon that found the following:

Almost 33% of respondents admit to having sacrificed mobile security to improve expediency and/or business performance. Of those, 38% say their organization is at significant risk from mobile threats. Further, 25% said that during the past year their company had experienced a security incident resulting in data loss or system downtime where mobile devices played a key role.

Meanwhile, the Verizon report also detailed the following types of mobile threats that we thought bankers might like to know:

Denial of service: Jamming of wireless communications, overloading networks with bogus traffic, ransomware, or loss/theft of device.

Geolocation: Gathering data on location, infringing on the privacy of the individual.

Information disclosure: Interception of data in transit, leakage or exfiltration of user, app or enterprise data, eavesdropping on voice or data communications, surreptitiously activating the phone's microphone or camera to spy on the user.

Spoofing: Email or text message pretending to be from a boss or colleague, fraudulent Wi-Fi access point, or cellular base station that mimics a legitimate one.

Tampering: Modifying data in transit, inserting tampered hardware or software into supply chain, repackaging legitimate app with malware, modifying network or device configuration (such as "jailbreaking" or "rooting" a phone).

Many factors also make mobile devices an appealing target. After all, there are more mobile devices, they have access to more data, and they are now critical to business operations. In this regard, the following practices could be a good start:

Apps: Reduce the risk of malicious and vulnerable applications by looking into creating a custom app store and vetting all apps that are added to it.

Segmentation: Improve device management by automating it as much as possible. This includes deploying mobile endpoint security/threat detection and implementing device segmentation, keeping personal and work data and applications separate.

Ambassadors: Train "security ambassadors" within the bank to act as champions for improved mobile security.

As mobile adoption continues, banks should continue to monitor changes to keep up. Having the right practices and processes in place, and refining them along the way, will ensure your bank and your customers remain well protected and less crunched by mobile cyber incidents.

HEDGING SERVICES FOR COMMUNITY BANKS

Community bankers seeing long-term fixed rate demand from business clients can transform payments into a floating rate on their books using Borrowers' Loan Protection (BLP). Contact us today for more information.