For the first time ever, studies reveal CONSUMERS AND BUSINESSES PREFER SECURITY OVER CONVENIENCE.

A 2018 survey conducted by IBM, found that 74 percent of respondents prefer security over convenience when it comes to their online financial accounts. Based on findings in the report, mobile and web users are more aware of the data breaches that are happening to companies and consumers alike. In another study, 79 percent of consumers choose retailers based on their cyber security credentials and 40 percent of consumers would be willing to increase their spend 20 percent or more if their primary retailer gave them certain assurances which built their trust.

As mobile online activities hit record highs, answer the growing demand for security by adding EndpointLock Keystroke Encryption to every smartphone and tablet.

EndpointLock™
Desktop and Mobile Security

AS MOBILE USAGE SOARS ...SO DOES THE RISKS

- 76% of people now use their mobile device for banking
- 79% of people have used their smartphone for shopping online
- 80% of businesses have adopted BYOD (Bring Your Own Device)
- Mobile Malware tripled in two years from 10 million to 30 million
- 67% of organizations had a data breach happen when an employee used their mobile phone to access the company's data.

PROBLEM:

KEYLOGGING SPYWARE is a main component of malware used to steal identity and credentials from a user's device, helping to advance the breach.

Keylogging spyware has become a problem in mobile security that is global in scope for both consumers and businesses alike. Keyloggers steal everything typed into the device including passwords, banking and credit card information. The spyware is secretly downloaded to a mobile smart phone or tablet when clicking on infected links inside emails, texts, social media and web pages and can also be embedded inside infected apps. The practice of tricking unsuspecting victims into clicking on links that look legitimate is called "phishing". According to recent reports, phishing was found in 90% of breaches and 95% of all phishing attempts that led to a breach were followed by software installation, including keyloggers, which are typically a main component in malware. Despite major advances in cyber security, news outlets consistently report about data breaches every day.

As consumers and businesses increasingly choose to use their mobile devices for e-commerce, online banking and for accessing sensitive data, the security risks multiply exponentially and cybercriminals are now focusing their efforts on exploiting mobile vulnerabilities. Unfortunately, keyloggers are difficult to detect by traditional anti-virus, even if these programs are up-to-date. For this reason, keyloggers remain on the device for months and sometimes years stealing every keystroke.

EndpointLock™
Desktop and Mobile Security

CONSUMERS:

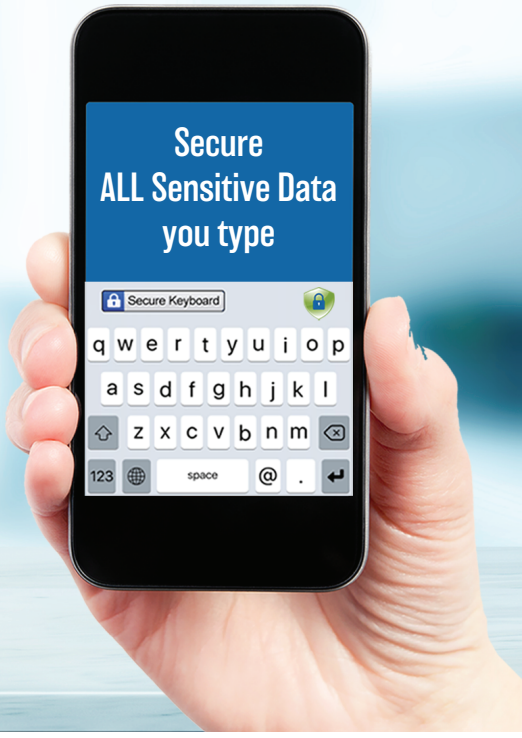
For consumers, having a keylogger infect their device means they are at risk for identity theft, which has reached epidemic proportions. In fact, there has been a 125% increase in identity theft over the last decade, account takeovers tripled in the last year and new account fraud rose by 70%.

BUSINESS:

For both the modern-day enterprise or small business, who has almost fully embraced BYOD (Bring your own device) and is regularly accessing sensitive company data, having a keylogger on their device could mean putting their company at risk of a major data breach. With the advent of Cloud Computing, you can now log into your company network from any place at any time, using any device. Today, over 50% of employees are working remotely for at least half of their work week.

Solution Brief

STEP UP MOBILE SECURITY WITH ENDPOINTLOCK SECURE KEYBOARD



SOLUTION:

The ONLY SOLUTION to stop zero-day keylogging spyware installed on a device.

EndpointLock for Mobile blocks keyloggers even if they have already been downloaded to the device and are able to evade anti-virus. Toggle back and forth, to use the Secure Keyboard whenever PII (personal identifying information) and other sensitive data such as login credentials are being entered.

PROTECT YOUR CUSTOMERS WHERE IDENTITY THEFT BEGINS:

Last year, credit card fraud was the most common form of identity theft. Visa, Mastercard, American Express, credit card issuers and online retailers have stepped up their security, by verifying and protecting customers. However, if a keylogger has infected the user's device, login credentials and credit card information are captured before they ever have a chance to be verified or pass through SSL/TLS protocol.

The mobile carrier provides a common link for every step in the online activity chain from the time new banking and shopping accounts are provisioned, through to the transaction. With EndpointLock pre-installed on every mobile smartphone and tablet, you can be the first link in the security chain protecting ALL keystrokes with a new security protocol, KTLS (Keystroke Transport Layer Security).

SECURE THESE ONLINE ACTIVITIES:

FOR CONSUMERS:

- Online Banking and Shopping
- Typing Emails and Texts
- Filling out Personal Health information
- Applying for Credit
- Account Provisioning

FOR BUSINESS:

- Business Banking
- Logging into a Network
- Working Remotely
- Entering Customer PII (Personal Identifying Information)

References:
1. https://www.techrepublic.com/article/ibm-security-report-security-now-outweighs-convenience/
2. https://www.teiss.co.uk/news/consumers-retailers-data-security/
3. https://thefinancialbrand.com/73785/banking-digital-payments-ing-paypal-credit-debit-cards-p2p-trends/
4. https://www.outerboxdesign.com/web-design-articles/mobile-ecommerce-statistics
5. https://securityintelligence.com/news/new-fraud-statistics-show-rising-volume-of-identity-theft/
6. https://www.forbes.com/sites/elenakvochko/2015/08/14/has-byod-become-inevitable/#4eb7615c3998
7. https://heimdalsecurity.com/blog/smartphone-security-guide-keep-your-phone-data-safe/
8. https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

EndpointLock™
Desktop and Mobile Security