G DATA

TRUST IN
GERMAN
SICHERHEIT

G DATA
WHITEPAPER

THE RISKS WHEN BANKING AND SHOPPING ONLINE

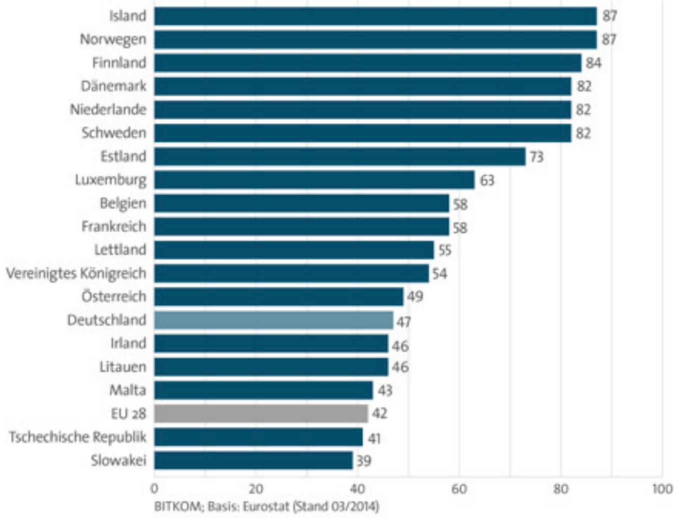
CONTENTS

MOTIVATION

Financial gain has long been the key motivator of highly professional cyber criminals and globally organized groups of hackers. Therefore it will be of no surprise that the growing number of online banking users continues to represent one of the most important targets of attack. What can promise more profit than siphoning off money being moved on the Internet directly at source?

According to the industry association BITKOM, the number of online banking users in Germany has risen from 27 million in 2011 to 37 million in 2014. That is 47 percent of all Internet users aged between 14 and 74. Among 14 to 29 year olds, the proportion is 70 percent, and among 30 to 49 year olds it is 71 percent. [1,2]

Anteil der E-Banking-Nutzer[1], 2013 (in %)



BITKOM; Basis: Eurostat (Stand 03/2014)
[1] Prozentanteil der Personen, die das Internet für Internet-Banking genutzt haben

Germany is in the middle ground in Europe when it comes to the proportion of online banking users. (Source: BITKOM)

According to the Federal Criminal Police Office (Bundeskriminalamt – BKA), 16.4 million euros was the amount that cyber criminals in Germany got their hands on from attacks on this group of users in 2013. However, the BKA estimates the actual damages are significantly higher – 180 million euros – as only around 10 percent of all successful cyber attacks are ever reported. On average, the thieves stole 4,000 euros per case. The State Criminal Police Office in Bavaria estimates the average amount to be even higher, at 5,000 euros.[3]

The "Online Banking 2014 - Security pays!" study produced by TNS Infratest under contract to IT service provider Fiducia and Initiative D21, reports that around two percent of users surveyed have at some time suffered damages when banking online. Furthermore, 17 percent reported that such an incident has occurred in their direct environment.[4, 5]

Despite new security measures when banking online, there is still a relatively high probability of becoming a victim of an attack and losing a lot of money as a result. However, the attack methods have fundamentally changed in recent years. Originally, social engineering methods such as phishing were used, whereby users were tricked into giving out the required access data and TAN numbers for account transactions. Nowadays current security methods always include two-way authorization and a user check, requiring that attack methods are more complexed.[6] Without exception, they use highly specialized malware programs and require alertness on the part of the user and specialized security solutions to fend them off. Both Windows PCs and mobile devices (which are being used more and more for online banking or two-way authorization) are increasingly being affected in this way.[7]

[1] http://www.bitkom.org/de/markt_statistik/64034_65226.aspx
[2] http://www.bitkom.org/de/markt_statistik/64034_80365.aspx
[3] http://www.heise.de/ct/ausgabe/2014-25-Millionenschaeden-durch-Angriffe-aufs-Online-Banking-2450695.html
[4] http://www.tagesspiegel.de/medien/digitale-welt/online-banking-angriffe-auf-den-digitalen-geldbeutel-nehmen-zu/10034102.html
[5] http://www.initiatived21.de/wp-content/uploads/2014/07/d21_fiducia_studie_onlinebanking_2014.pdf
[6] http://www.handelsblatt.com/finanzen/steuern-recht/recht/ratgeber-hintergrund/sicherheitsluecken-vorsicht-beim-online-banking/9434420.html
[7] http://www.bitkom.org/de/publikationen/38337_81169.aspx

CURRENT AUTHORIZATION PROCESSES FOR ONLINE BANKING

Basically there are two completely different methods for online banking: via the HBCI/FinTS protocol and associated client software, or via the web browser and use of a web portal. As the proportion of attacks on HBCI/FinTS clients is dwindling and the vast majority of users carry out their banking transactions using the web browser, the former process will be left out of this observation.

The basis for all authorization processes for web-based online banking is the separation of account access into user identification via access password/PIN and the release of account transactions via transaction numbers (TANs). These transaction numbers were originally sent to the user by post as a list and could be used in any sequence to trigger transfers, etc. If an attacker knew just one of the valid (i.e. unused) TANs along with the access data, he had all the data required to carry out a fraudulent transfer. Current processes therefore rely on tightened criteria for the validity of a transaction number.

I-TAN

With the iTAN process only a TAN in a randomly determined position is valid, and no longer any TAN from the mailed list. Authorization cannot be carried without knowing the entire list – or a large part of it. The disadvantage of this is that an attacker can get hold of the required information for triggering transfers by skillful phishing of multiple TANs or by stealing the list.

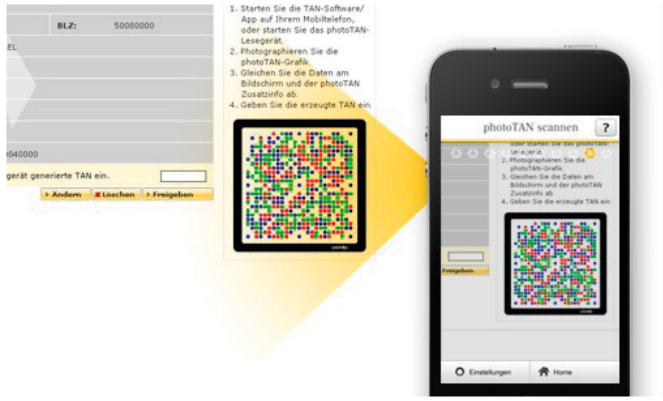
SMS-TAN/M-TAN

The smsTAN/mTAN process works without a predefined list and additionally introduces a second transfer path when generating a valid TAN. The user sets up a transfer or other account transaction online; the bank then sends a TAN valid only for this transaction plus the target account number and amount via SMS to the customer's mobile phone. Linking the amount, the target account and TAN, and giving the customer the option of checking the transfer data make it difficult for a valid TAN to be stolen compared to the iTAN process. However, there is a risk of the SMS messages being intercepted or forwarded to another mobile phone by malware.

PHOTO-TAN/PUSH-TAN

Unlike the smsTAN method, photoTAN and pushTAN do not use SMS messages. With the photoTAN process, a coloured graphic is displayed on the PC screen after a transaction has been set up; this is photographed using the mobile phone's camera and converted into a TAN by a banking app on the telephone. Optionally a reader can also interpret the graphic, which is a more secure alternative because of the smaller risk of manipulation.

The pushTAN process sends the transaction data set up online over the Internet to the banking app on the user's mobile phone. Here it can be checked and a TAN number generated from it. Both photoTAN and pushTAN block the route for attackers trying to access valid TANs by intercepting SMS messages. However, the banking apps used on the mobile phone can also become the target for attacks.



1. Starten Sie die TAN-Software/ App auf Ihrem Mobiltelefon, oder starten Sie das photoTAN-Lesegerät.
2. Photographieren Sie die photoTAN-Grafik.
3. Gleichen Sie die Daten am Bildschirm und der photoTAN Zusatzinfo ab.
4. Geben Sie die erzeugte TAN ein.

With the photoTAN process a TAN is generated by reading an encrypted graphic on the PC screen. (Source: Commerzbank)

CHIP-TAN/E-TAN/SMART-TAN

The authorization process generally referred to as chipTAN does not use the mobile phone but an electronic TAN generator for generating a valid transaction number. Depending on the format, the method by which the TAN is generated differs:

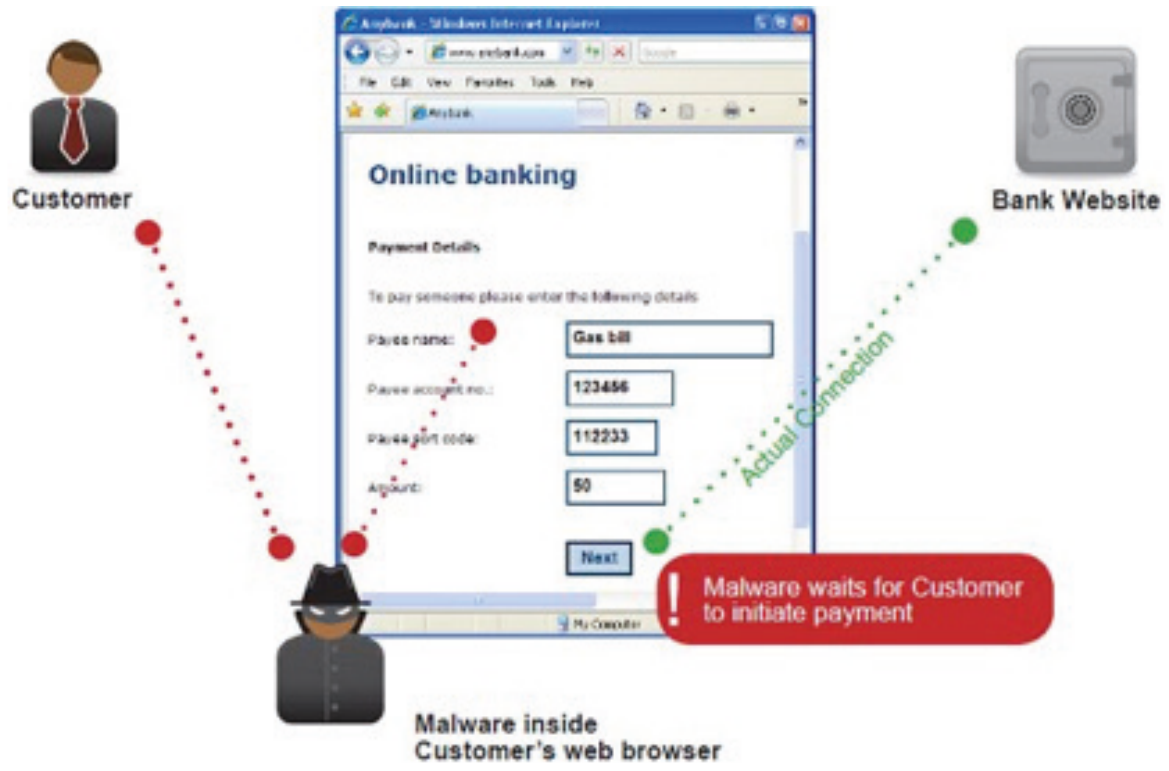
- With the smartTAN process, a customer card belonging to the account (Maestro/ec/V Pay card) just needs to be inserted into the TAN generator to be able to generate valid TANs at the push of a button. The weakness with this is that theft of the customer card enables an attacker to generate valid TANs. However, blocking the card can thwart an attempted attack.
- An eTAN generator is personalized to the customer and generates the TAN number using a secret key, the time and the transfer recipient's account number. This is keyed in by the customer on the device's numeric keypad. Many banking institutes also use a control number generated by the web portal instead of the recipient's account number. However, this is susceptible to manipulation.
- The chipTAN process involves using an electronic TAN generator, into which a card is inserted, and a numeric keypad. The customer's card is first inserted into the device and the TAN is then generated in various ways depending on the institute. With some banks the customer enters a start code, the recipient's account number and the amount via the keyboard (manual chipTAN). With many savings banks and cooperative banks a graphic consisting of five black and white flickering bars ("flicker code") is displayed on the computer screen that the TAN generator reads using optical sensors. The target account number and the amount are also transferred in this way, so the customer can check them prior to generating the TAN on the device. This process is currently considered to be the most secure. [7]

[7] http://www.bitkom.org/de/publikationen/38337_81169.aspx

ATTACK METHODS

Linking the transaction data and TAN and use of a second transfer method unconnected with the PC for generating valid TANs has made it much harder for cyber criminals to access the data for carrying out a transfer. It is no longer enough to get one's hands on the account access data and an unused TAN or list of TANs. Online theft requires a TAN that matches the unlawful transfer. Therefore what all effective methods of attack have in common is manipulation of the transfer data before the TAN is generated.

For this purpose, cyber criminals rely on highly specialized Trojans, which are among the most advanced malware programs of all. Generally the Trojans are precisely adapted to a range of international online banking portals using add-ons called web injects. These add-ons access popular web browsers (Internet Explorer, Firefox, Google Chrome, Opera) and manipulate the communication between the PC and the bank's computer. The encrypted communication between the user's computer and the bank's server is bypassed when doing so, as all the data sent has already been modified before or after the encryption in the browser. The "man-in-the-middle" attack, which interrupts and manipulates the communication chain, becomes a "man-in-the-browser" attack, elegantly circumventing the barrier of encrypted communication.[3]



Online banking

Payment Details

To pay someone please enter the following details

Payee name: Gas bill

Payee account no.: 123456

Payee sort code: 112233

Amount: 50

Next
Customer
Bank Website
Actual Connection
Malware waits for Customer to initiate payment
Malware inside Customer's web browser

Current malware infiltrates the victim's browser and manipulates the bank data before and after encryption. (Source: securityaffairs.co)

[3] http://www.heise.de/ct/ausgabe/2014-25-Millionenschaeden-durch-Angriffe-aufs-Online-Banking-2450695.html

THE ATTACK ITSELF CAN TAKE PLACE WITH VARIOUS LEVELS OF COMPLEXITY

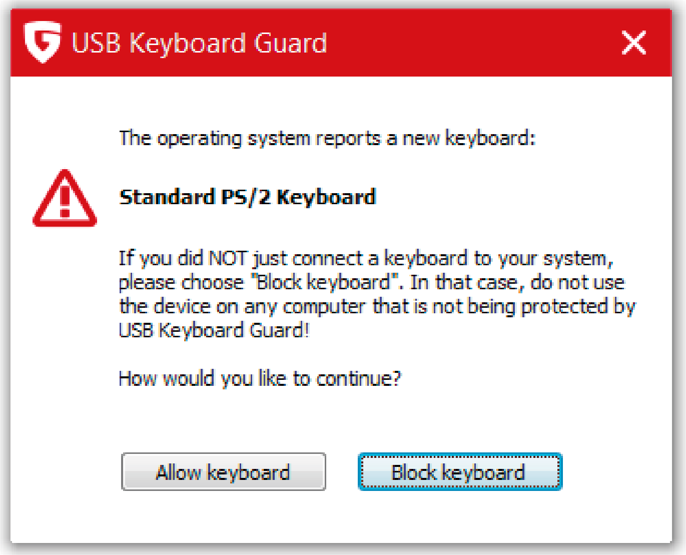
- In the simplest case, the malware pretends to the user that there is supposedly a "return transfer", "test transfer", "security check", "conversion to the IBAN process" or similar. The user is then supposed to generate and enter a TAN. The generated TAN matches a transfer running simultaneously in the background on the criminal's account. The advantage of this process is that, because of the apparent legitimacy and the transfer being triggered by the customer, all of the common authorization procedures are bypassed, including the chipTAN. The disadvantage of this is that an informed customer will immediately recognize the attempted fraud.
- The customer's mobile number and his mobile phone's operating system are requested by including an additional text field on the bank's login page. A link for downloading supposed security software leads him to infect his mobile phone with additional malware. The attackers can now control access to the bank account and can intercept TAN numbers sent via SMS. This gives them the ability to carry out transfers themselves. Depending on the authorization process, malware for requesting/forwarding photoTANs or pushTANs are also conceivable.
- The malware manipulates the transfer data in the background without the customer noticingand this modified data is used to generate a valid TAN. The fraud is only discovered if the user rechecks the target data for the transfer prior to entering the TAN.
- By using the personal data requested by the malware, the attackers can order a second SIM card from the customer's mobile phone provider. This enables them to receive SMS for sending transaction numbers from their own mobile phones and carry out their own transfers.
- Especially well organized groups have even manipulated the bank's hotline number to redirect calls from suspicious customers to their own call center. The "bank employees" there explained to the victims that the malware's displays were harmless and advised them to follow the instructions on the screen.[3]

[3] http://www.heise.de/ct/ausgabe/2014-25-Millionenschaeden-durch-Angriffe-aufs-Online-Banking-2450695.html

HOW G DATA BANKGUARD PROTECTS AGAINST "MAN-IN-THE-BROWSER" ATTACKS

The first line of defence against banking Trojans is virus detection by the installed security solution. If the malware's signature is known, it is identified when downloaded and rendered harmless.

If the detection fails due to the malware being unknown, G DATA BankGuard protects the browser against manipulation that use web injects. With online banking – as with encrypted access to an online shop – the connection to the bank's computer is set up via a browser library located in the main memory. This is where the data from the encrypted SSL connection is decoded. G DATA BankGuard compares the version of the library currently stored in the main memory with a trustworthy copy generated by BankGuard itself. If any deviation is detected, a warning message is displayed warning the user of the risk. The browser session is forced to close immediately and is cleaned of the detected banking Trojan. This effectively prevents the malware from manipulating the data.



The operating system reports a new keyboard:

Standard PS/2 Keyboard

If you did NOT just connect a keyboard to your system, please choose "Block keyboard". In that case, do not use the device on any computer that is not being protected by USB Keyboard Guard!

How would you like to continue?

G DATA BankGuard is an integral part of all G DATA security solutions for Windows (ANTIVIRUS, INTERNET SECURITY, TOTAL PROTECTION) and has an option in the program settings to enable it to be switched on and off easily.

G DATA INTERNET SECURITY FOR ANDROID ALSO SECURES THE TRANSFER OF TRANSACTION NUMBERS

G DATA INTERNET SECURITY FOR ANDROID can effectively increase the level of protection when the bank customer uses one of the authorization processes for mobile phones. The program analyzes the permissions of all the installed apps and in this way can recognize previously unknown phishing apps. Furthermore, the reliable malware scanner identifies the signatures of known malware among downloads and apps in the device memory. This prevents SMS messages or TANs generated by apps from being intercepted in the event of an online banking attack.

REFERENCES

1. BITKOM: Eurostat eBanking Usage Statistics (German)
http://www.bitkom.org/de/markt_statistik/64034_65226.aspx

2. BITKOM: 37 million Germans use online banking (German)
http://www.bitkom.org/de/markt_statistik/64034_80365.aspx

3. Uli Ries: Bankraub Digital, c't edition 25/2014, page 76 (German)
http://www.heise.de/ct/ausgabe/2014-25-Millionenschaeden-durch-Angriffe-aufs-Online-Banking-2450695.html

4. Kurt Sagatz: Attacks on digital wallets increase (German)
http://www.tagesspiegel.de/medien/digitale-welt/online-banking-angriffe-auf-den-digitalen-geldbeutel-nehmen-zu/10034102.html

5. Initiative 21 study: "Online Banking – Security pays" (German)
http://www.initiatived21.de/wp-content/uploads/2014/07/d21_fiducia_studie_onlinebanking_2014.pdf

6. Sara Zinnecker: Caution when Online Banking (German)
http://www.handelsblatt.com/finanzen/steuern-recht/recht/ratgeber-hintergrund/sicherheitsluecken-vorsicht-beim-online-banking/9434420.html

7. BITKOM: Online Banking Guidelines (German)
http://www.bitkom.org/de/publikationen/38337_81169.aspx

TRUST IN
GERMAN
SICHERHEIT