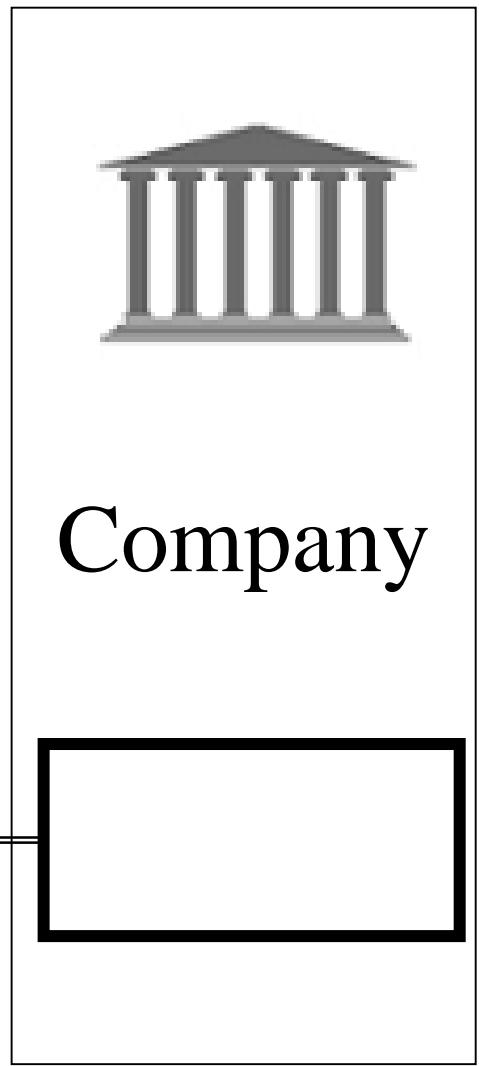
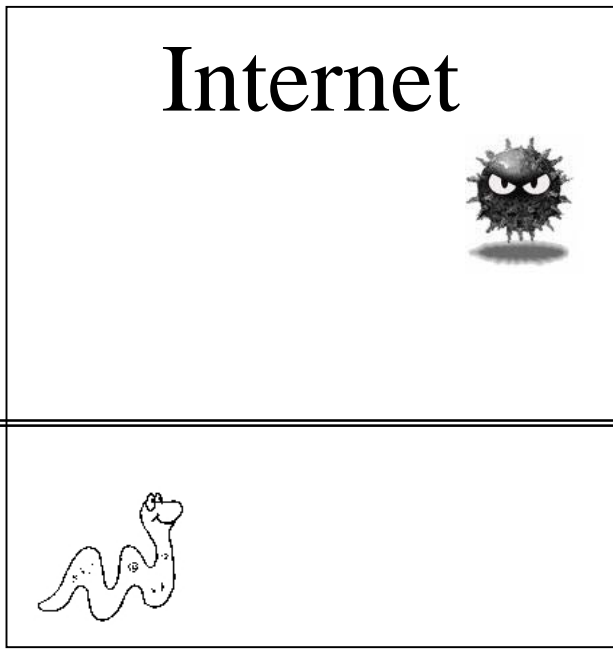
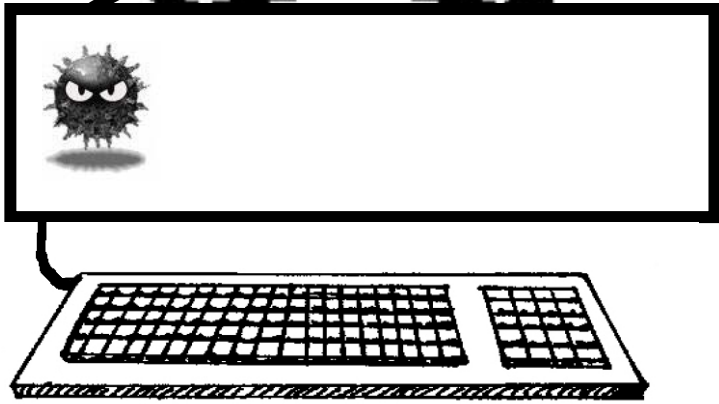
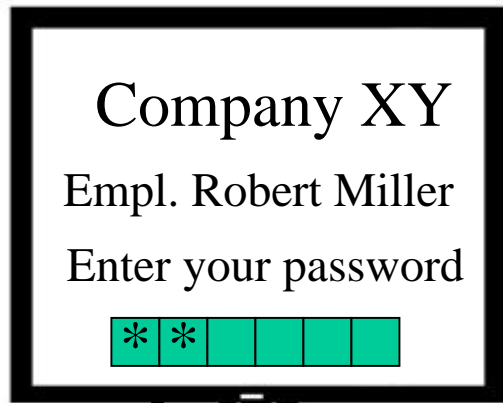


Secure Access to Enterprise Accounts

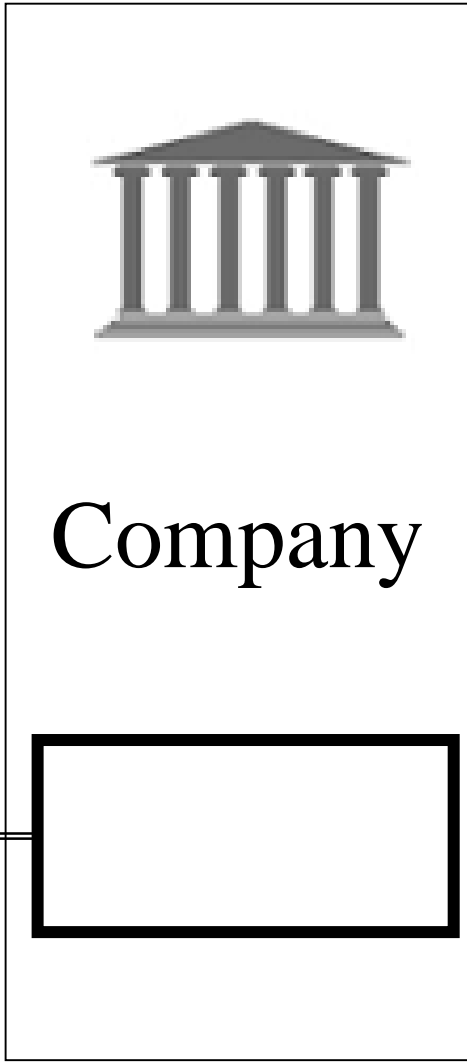
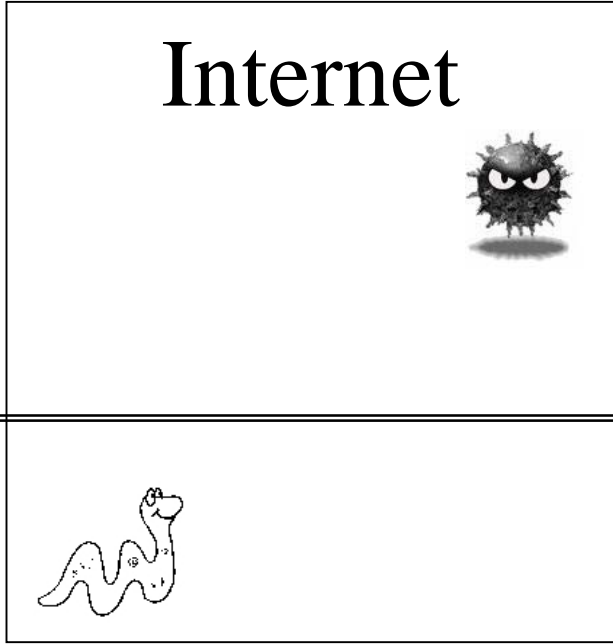
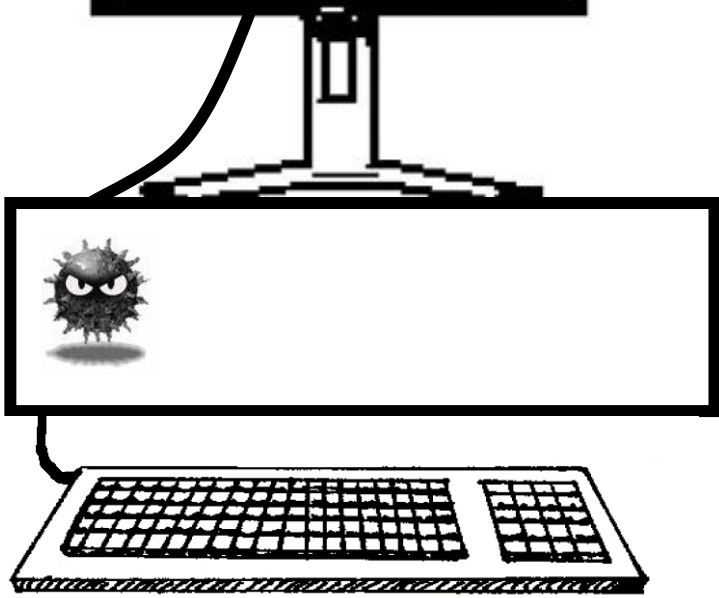
Bernd Borchert, Heidelberg, November 2008

Enterprise Account secured by PIN

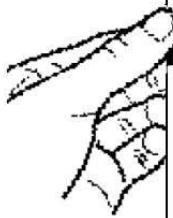


Enterprise Account secured by Token

Company XY
Empl. Robert Miller
Enter your code:
* *
Enter your password



Permutation PIN



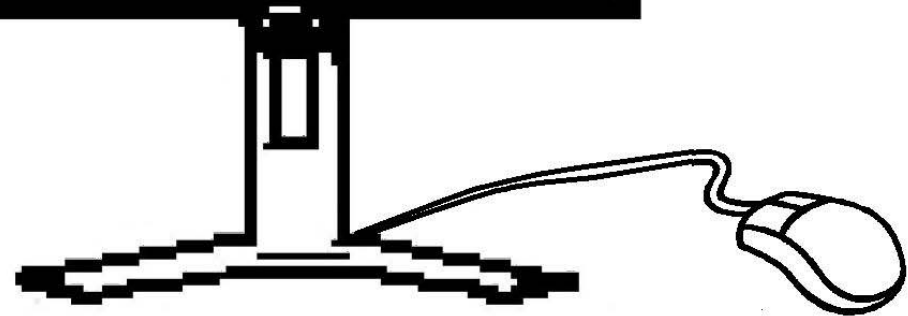

Nr. 1	5 7 0 8 4	6 1 3 2 9
Nr. 2	1 9 2 3 7	6 0 5 8 4
Nr. 3	0 2 5 4 6	7 8 1 9 3
Nr. 4	0 5 6 7 3	9 8 4 1 2
Nr. 5	3 4 5 2 0	8 6 1 7 9
Nr. 6	7 0 1 4 9	6 2 5 8 3
Nr. 7	8 4 5 1 7	9 3 0 6 2

XY-Bank (online access)

Account #1234567

Please enter your PIN: (via mouse)

Nr. 3



XY-Bank (online access)

Account #1234567

Please enter your PIN: (via mouse)

Nr. 3

Confirm

Correct

Cancel

Nr. 3 0 2 5 4 6 7 8 1 9 3

Nr. 4 0 5 6 7 3 9 8 4 1 2

Nr. 5 3 4 5 2 0 8 6 1 7 9

Nr. 6 7 0 1 4 9 6 2 5 8 3

Nr. 7 8 4 5 1 7 9 3 0 6 2



XY-Bank (online access)

Account #1234567

Please enter your PIN: (via mouse)

Nr. 3

* _ _ _

Confirm

Correct

Cancel

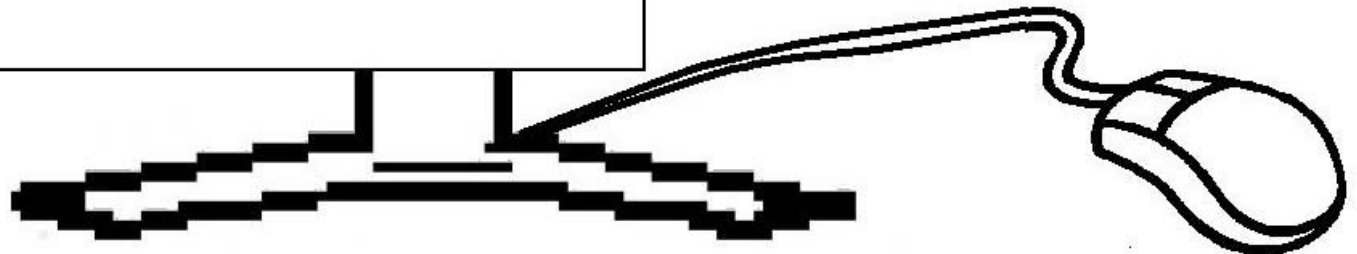
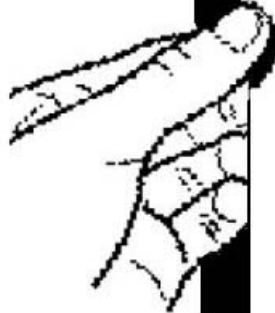
Nr. 3 0 2 5 4 6 7 8 1 9 3

Nr. 4 0 5 6 7 3 9 8 4 1 2

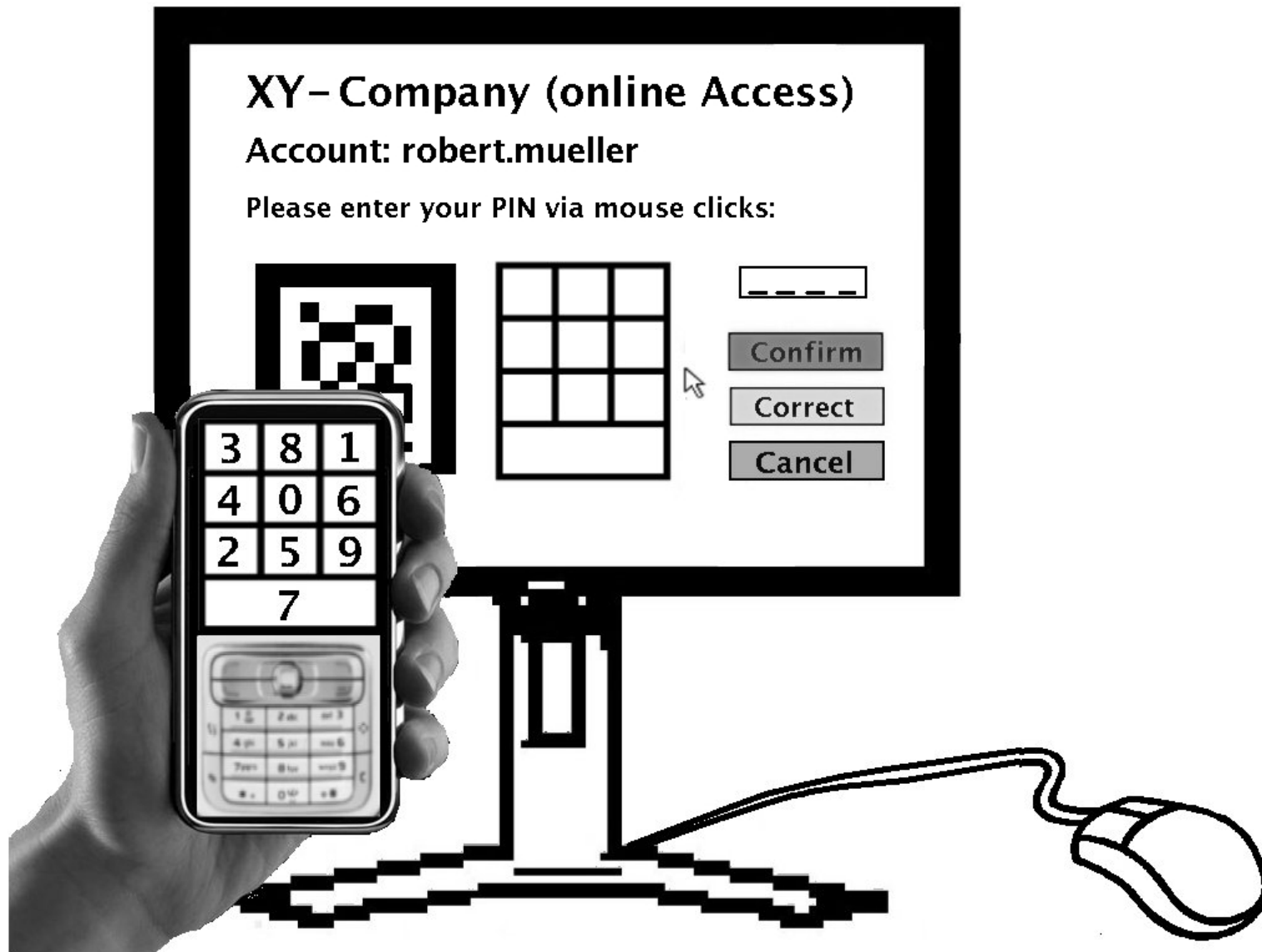
Nr. 5 3 4 5 2 0 8 6 1 7 9

Nr. 6 7 0 1 4 9 6 2 5 8 3

Nr. 7 8 4 5 1 7 9 3 0 6 2



Fotohandy-PIN





Demonstration des Fotohandy-PIN Verfahrens

Das Fotohandy-PIN Verfahren hat den Zweck, Trojaner davon abzuhalten, die PIN bzw. das Passwort zu einem Online Account (Email, Bank, Game-Server, etc.) abzulesen. Ausserdem verhindert die Fotohandy-PIN das Fälschen von Transaktionen, z.B. bei einer Banküberweisung.

Sie benötigen ein Foto-Handy, auf dem das Fotohandy-PIN Programm installiert ist. Das Programm sowie eine Liste der unterstützten Handys finden Sie auf der [Download-Seite](#). Wenn Sie kein passendes Handy haben, können Sie zu Demonstrationszwecken ein simuliertes Handy aufrufen:

[Virtuelles Handy starten](#)

Fotografieren Sie mit dem Programm den 2D-Code auf dem Bildschirm. Das Handy zeigt Ihnen danach ein Nummernfeld mit vertauschten Ziffern. Geben Sie dann durch Klicken der entsprechenden Felder die PIN ein, und zwar auf dem leeren Nummernfeld auf dem Bildschirm (nicht auf dem Handy). Die PIN steht - für diese Demonstration - in der "Gedankenwolke" rechts neben dem leeren Nummernfeld. Unten auf dieser Seite finden Sie eine Video-Bedienungsanleitung.

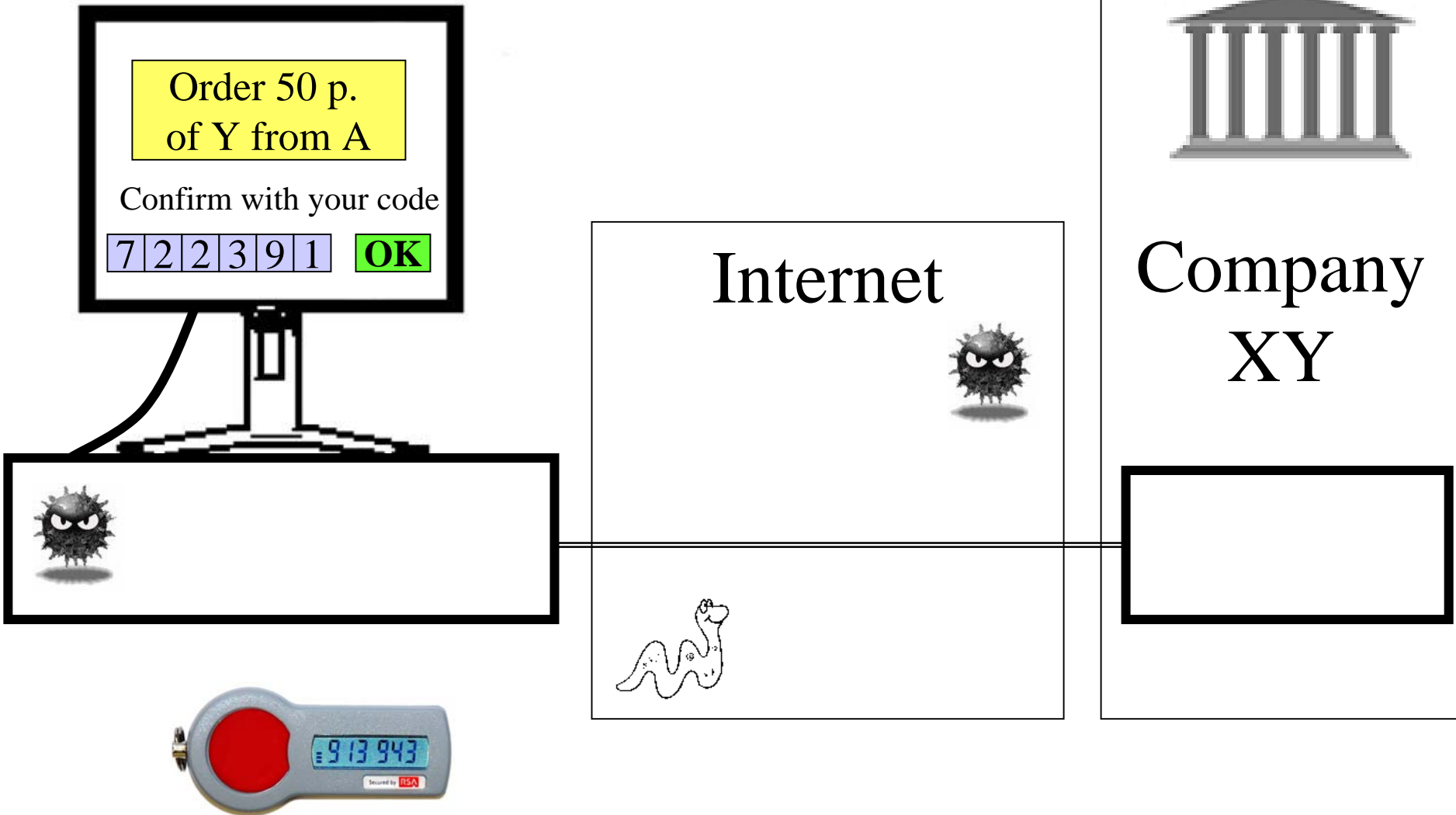
Bank XY, Konto 12121212. Bitte geben sie Ihre PIN ein:



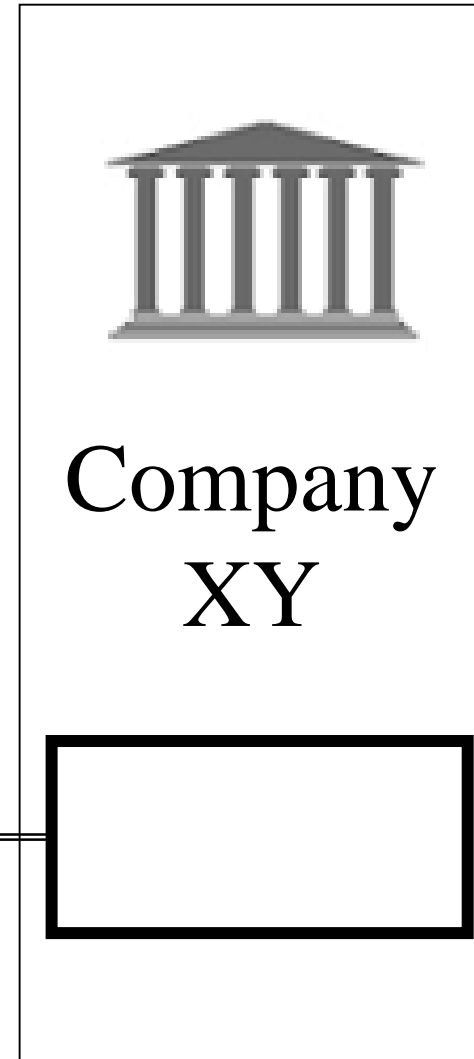
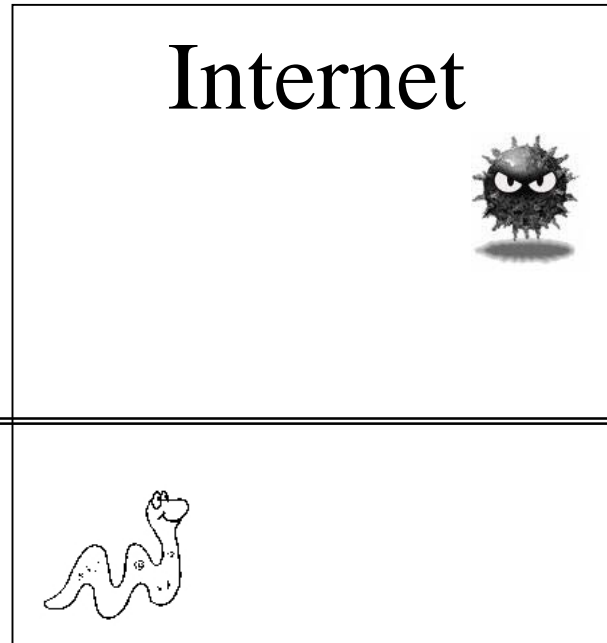
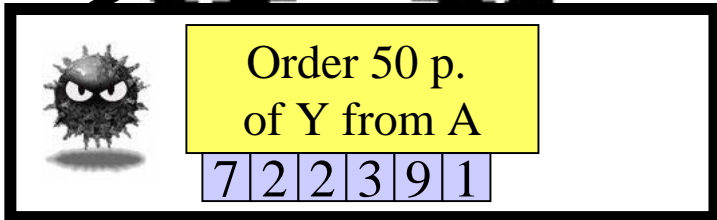
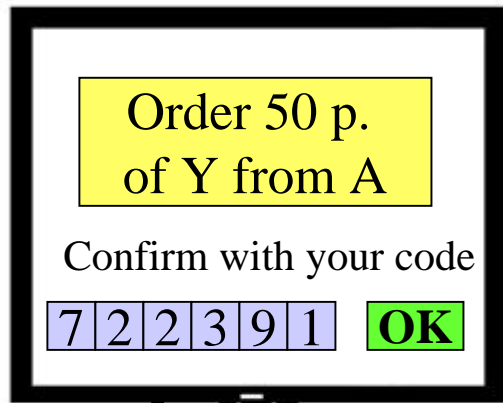


Warum verhindert dieses Verfahren das Abhören der PIN durch einen Trojaner auf Ihrem Rechner? Weil ein Trojaner nur die Positionen der Klicks in das leere Eingabefeld "sieht", er aber nicht weiß, was sie bedeuten.

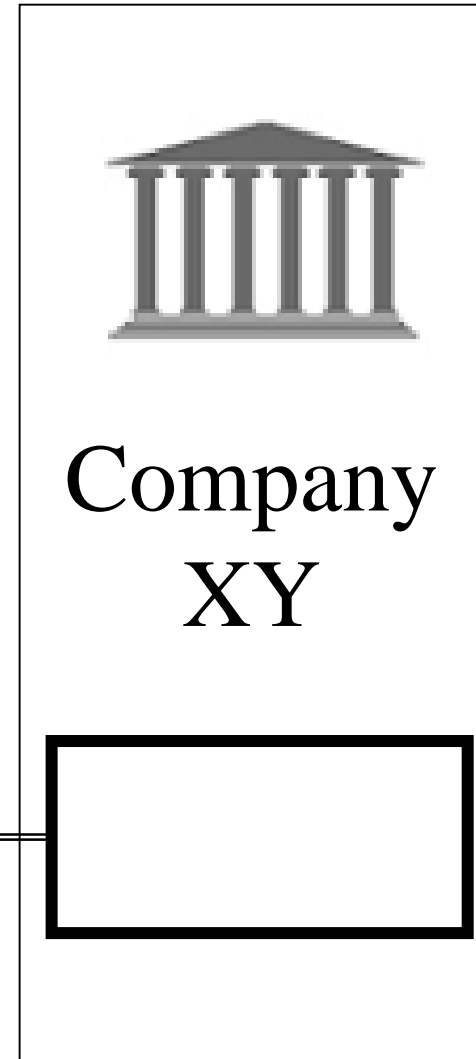
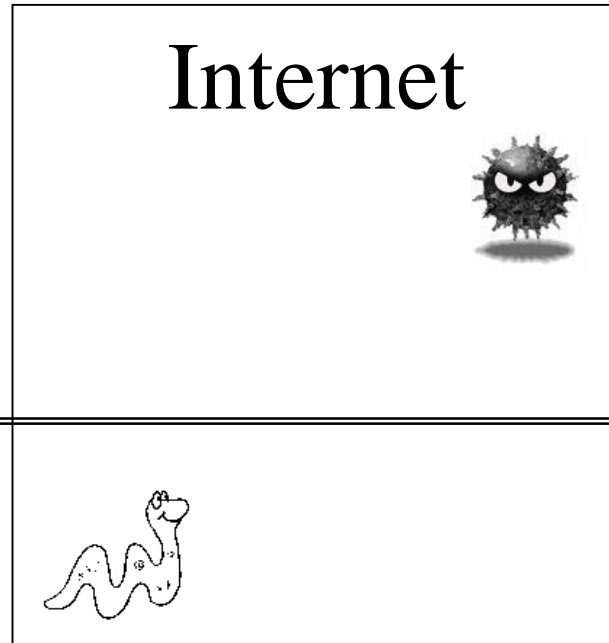
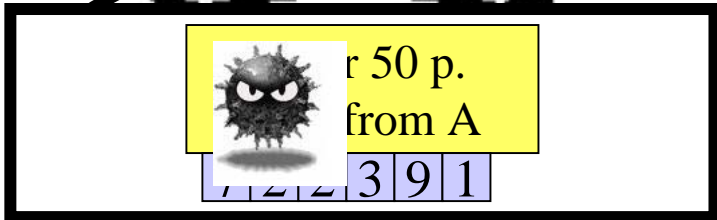
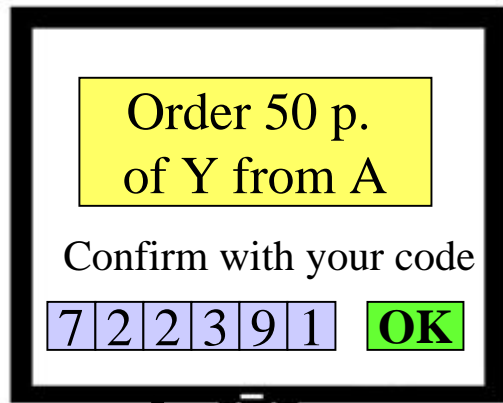
Transaction secured by token



Transaction secured by token



Transaction secured by token



Transaction secured by token

Order 50 p.
of Y from A

Confirm with your code

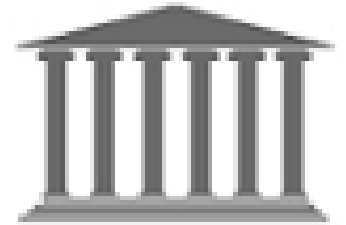
7 2 2 3 9 1 **OK**

Order 5000 p.
of Z from B

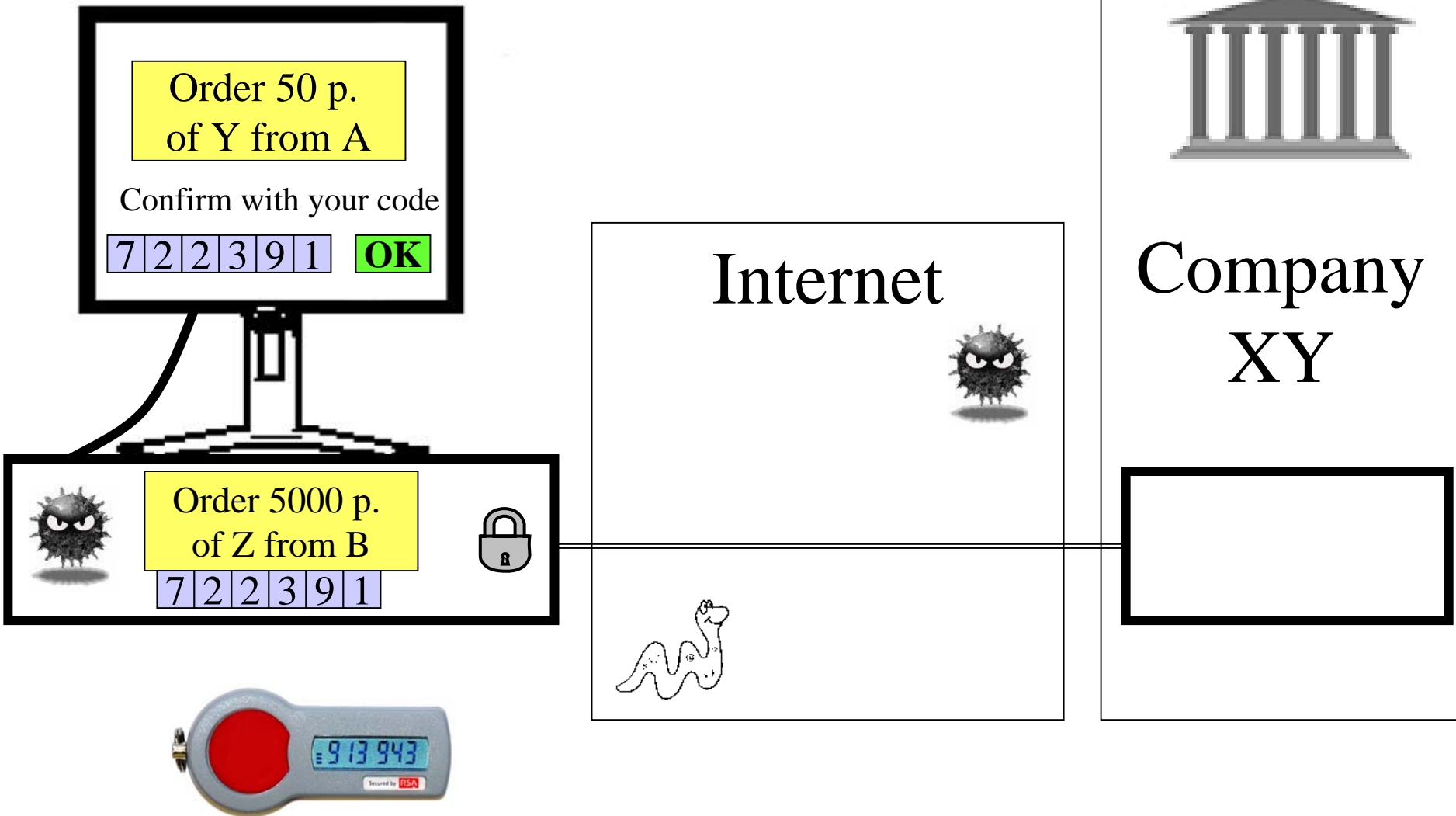
7 2 2 3 9 1

Internet

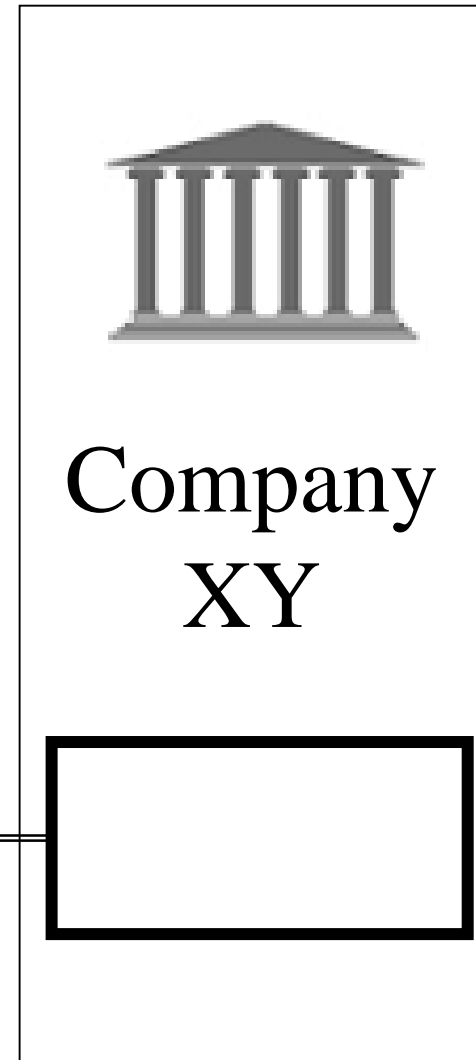
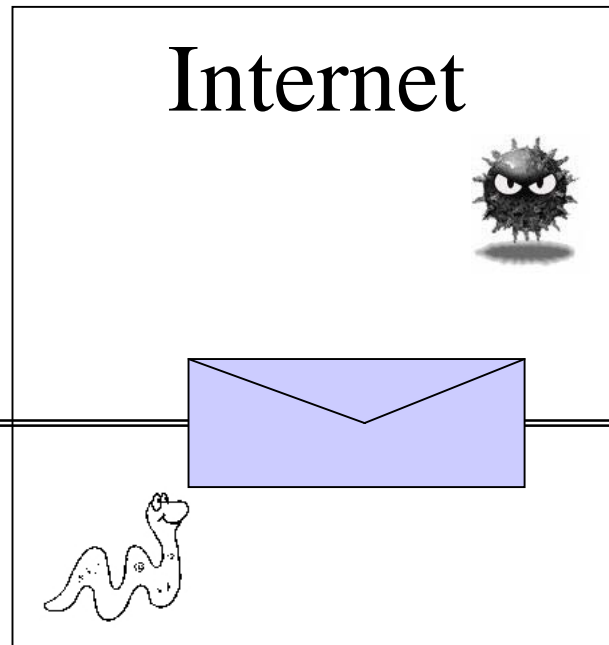
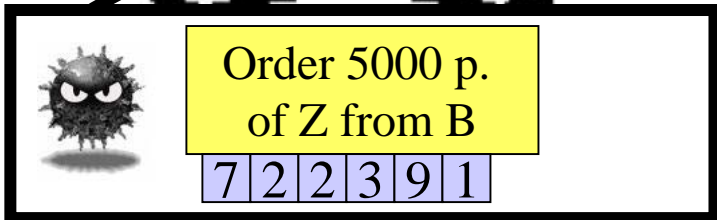
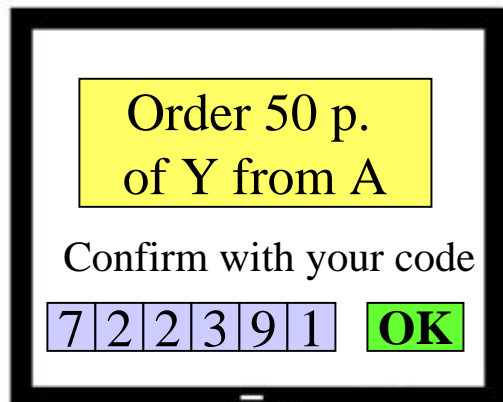
Company
XY



Transaction secured by token



Transaction secured by token




Transaction secured by token

Order 50 p.
of Y from A

Confirm with your code

7	2	2	3	9	1	OK
---	---	---	---	---	---	-----------

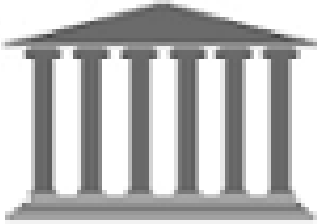




Order 5000 p.
of Z from B

7	2	2	3	9	1
---	---	---	---	---	---



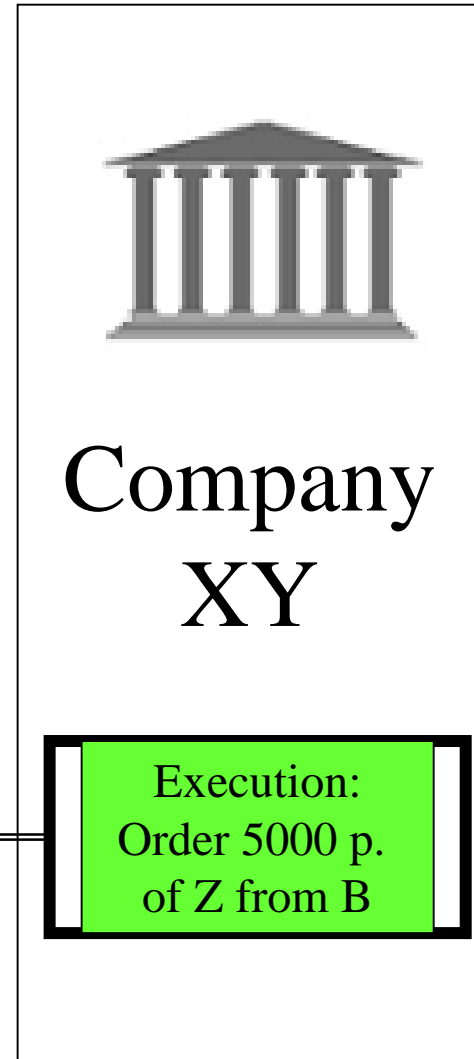
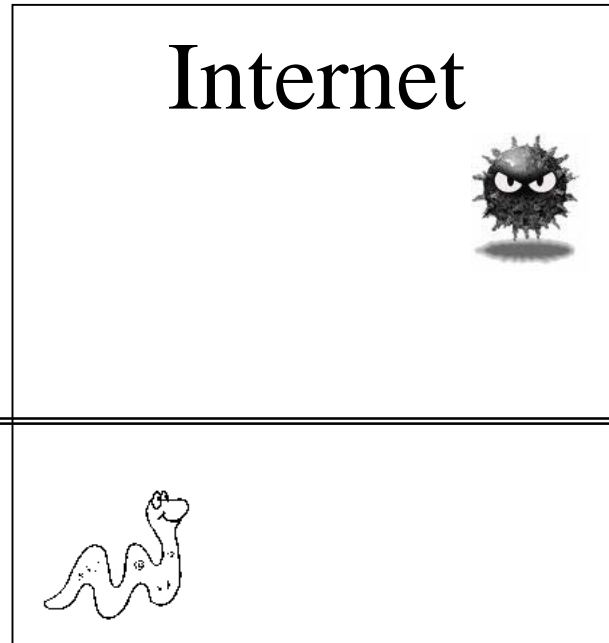
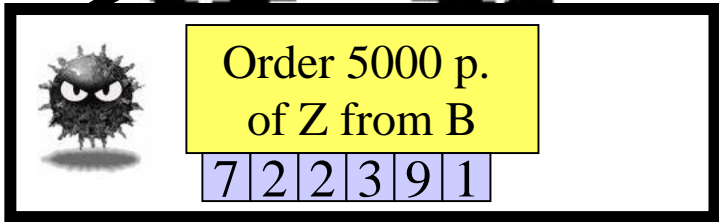
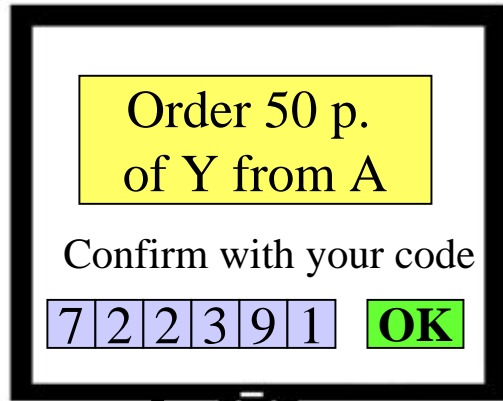
Internet



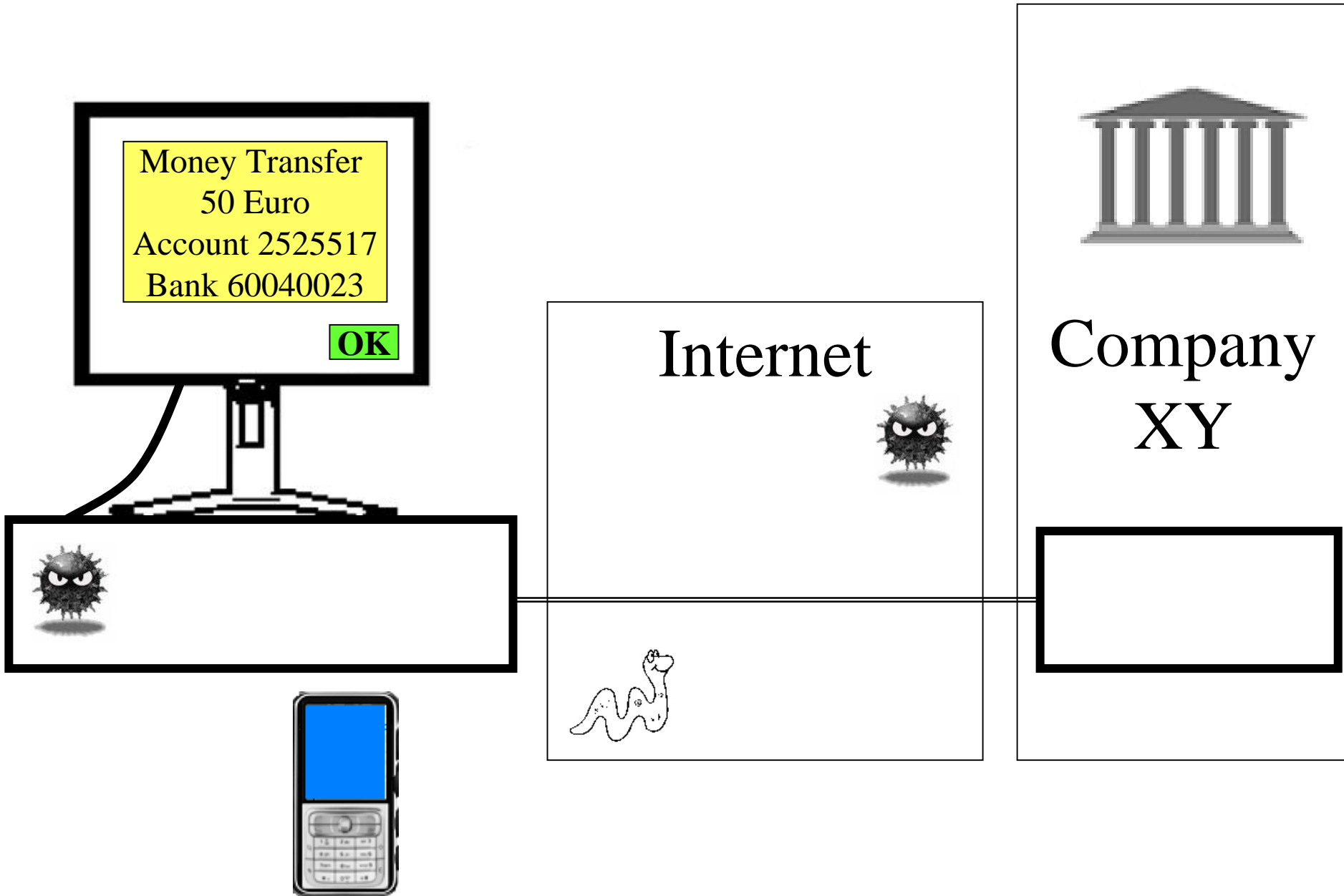
Company
XY

7	2	2	3	9	1
---	---	---	---	---	---

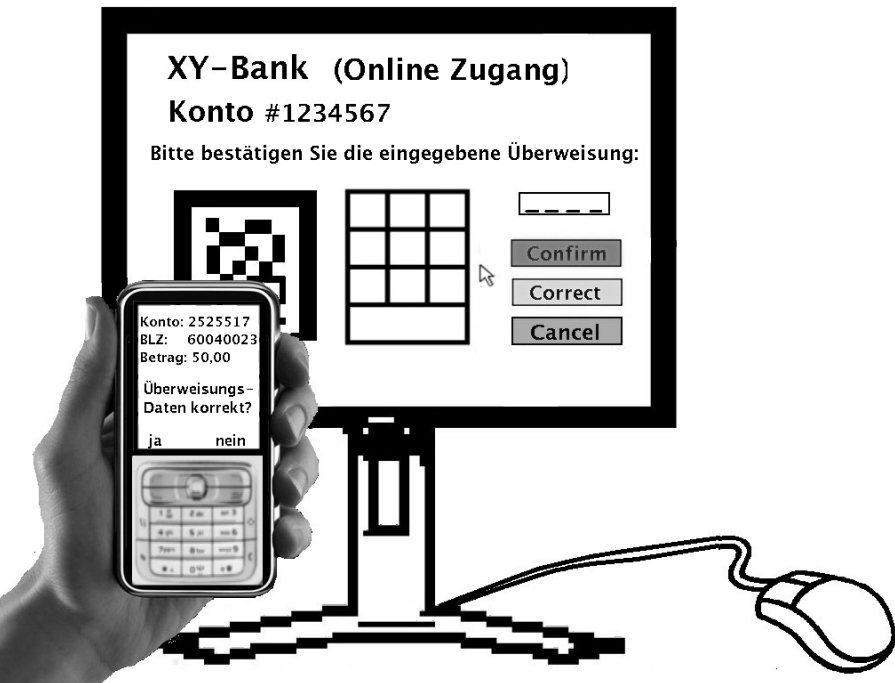
Transaction secured by token is INSECURE



Transaction secured by the camera phone



Transaction secured by the camera phone



XY Company

Employee Mueller

Please type number of item to be ordered

Nr. 3

Confirm

Correct

Cancel

Nr. 3 0 2 5 4 6 7 8 1 9 3

Nr. 4 0 5 6 7 3 9 8 4 1 2

Nr. 5 3 4 5 2 0 8 6 1 7 9

Nr. 6 7 0 1 4 9 6 2 5 8 3

Nr. 7 8 4 5 1 7 9 3 0 6 2



Summary

We presented a new method to secure enterprise accounts against

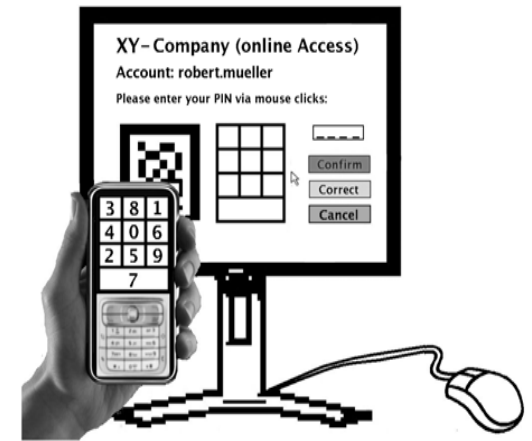
- identity theft (= password logging)
- manipulation of business transactions

executed by trojans on the computer the employee is using.

We have

- a low-tech version of the method using paper
- a high-tech version using the camera phone of the employee.

Both versions are secure. For both versions software prototypes exist. Patent applications are pending.



The new method has advantages compared to the established „Token“ method: Costs, usability, and secureness (transactions).

There are several 100 millions of enterprise accounts to be protected. Enterprises are willing to pay a higher price for secureness than for example email providers are willing to pay.