Phishing: Bitte nicht anbeissen!

Als versucht wurde, mittels Massenmails und gefälschter Webseiten die Zugangscodes der KundInnen einiger österreichischer Banken zu stehlen, wurde *Password Fishing*, kurz *Phishing*[1], plötzlich auch hierzulande als Bedrohung wahrgenommen. Dabei kämpft der gesamte eCommerce von Anfang an mit zwei Problemen.

Das erste: Die KundInnen misstrauen dem elektronischen Hokuspokus und shoppen und „banken“ nur zögerlich online. Das ist schade für die Firmen (schließlich ließen sich doch auf diese Weise Kosten sparen), und so begegneten sie dieser Herausforderung fachgerecht und nicht ohne Erfolg mit der Werbekeule.

Das andere Problem liegt tiefer und Fachleute wissen es schon längst: Das Misstrauen der technikfeindlichen eSkeptiker ist nicht ganz unberechtigt. Zwar haben – wie der Artikel *WWW + SSL = HTTPS* auf Seite 46 zeigt – die TechnikerInnen einiges unternommen, um elektronische Transaktionen sicher abwickeln zu können, doch der Faktor Mensch bleibt ein mitunter recht schwaches Glied in der Kette.

Die Rache der Benutzerfreundlichkeit

In ein Geschäft gehen, eine Wurstsemmel verlangen und ein paar Münzen hinlegen – das durchschaut jedes Kind, und allen Beteiligten ist wenigstens im Prinzip klar, worauf sie aufpassen müssen, um nicht über den Tisch gezogen zu werden. Dennoch finden BetrügerInnen immer wieder ein Opfer.

In der virtuellen Welt haben die intuitive Bedienbarkeit und die enorm gestiegene Benutzerfreundlichkeit zweierlei Erfolge gebracht: Jeder kann etwas mit dem Computer anfangen, und niemand weiß mehr, was er eigentlich tut. Wer hat schon eine Ahnung, was passiert, wenn wir auf der Telebanking-Webseite irgendwohin klicken? Wer kann sagen, worauf wir aufpassen müssen, um nicht übers Ohr gehauen zu werden? Nur ein verschworener Klüngel von Bitologen und Byte-Experten ist, wenn überhaupt, in der Lage, von sich aus die lauernden Gefahren zu überschauen und zu vermeiden.

Ergebnis: Nicht weil die Technik versagt, ist Internet-Betrug so einfach, sondern weil sie ihre AnwenderInnen beherrscht anstatt umgekehrt.

Das Kind nicht mit dem Bade ausschütten

Einerseits nicht der Paranoia zu verfallen und die ganze Computerei zum Teufel zu jagen, andererseits dennoch ein sozial verträgliches Maß an Sicherheit für die BenutzerInnen herzustellen, ist eine große Herausforderung, der wir alle uns jetzt stellen müssen.

Serverbetreiber und Softwarehersteller müssen, das versteht sich von selbst, ihre Systeme dem Stand der Technik entsprechend konzipieren und dafür sorgen, dass allfällige

1) Die Benennung erfolgte in Anlehnung an das in den frühen 90er-Jahren in Hacker-Kreisen übliche *Phreaking*, das von *Phone Freak* abgeleitet wurde.

Fehler unverzüglich behoben werden. Das ist der vergleichsweise einfache Teil.

Wesentlich komplizierter ist es, Rahmenbedingungen zu schaffen, die Sicherheit ermöglichen:

- Da neue Features neue Käufer anlocken und Geldverdienen das Ziel jeder Firma ist, werden gerne neue Funktionen erfunden. Dort allerdings, wo die Beherrschbarkeit und Sicherheit des Produkts gefährdet sind, müssen dem Featurismus Grenzen gesetzt werden. Ein Beispiel, das uns bereits viele Tränen gekostet hat: Die Möglichkeit, kinderleicht mit einem Mausklick aus einer eMail heraus neue Software zu installieren und auszuführen, hat sich als extrem ärgerliches und teures Feature erwiesen. Der Großteil aller Würmer, Viren und Trojaner – die heute zunehmend kriminellen Zwecken dienen[2)] und sich auch für Phishzüge vorzüglich eignen – kam so in die PCs, und dass das passieren musste, war abzusehen.

  Brauchbare Ansätze für einen diesbezüglichen Paradigmenwechsel sind leider rar. Auch Microsofts kommendes Betriebssystem Windows Vista, in dem Security als Feature vermarktet wird, dürfte sich in dieser Hinsicht eher als Marketing-Luftblase erweisen (siehe dazu den Artikel *Veni, vidi – und testete Vista!* auf Seite 18).

- Nur sehr zögerlich spricht sich in die Chefetagen durch, dass Sicherheit ein unternehmenskritischer Prozess ist, der bei Entscheidungen unbedingt berücksichtigt werden muss. Eine gesunde Balance zwischen der Technokratie paranoider Hacker[3)] und der Erfolgsorientiertheit bilanzfixierter Schlipsträger[4)] zu finden, erfordert einige Dialogbereitschaft zwischen diesen beiden Gruppen, die einander leider eher als natürliche Fressfeinde erleben dürften.

- Die BenutzerInnen müssen selbstverständlich über den richtigen und sicheren Umgang mit den Systemen, die sie verwenden sollen, Bescheid wissen. Dazu gehört ein ausreichendes Verständnis von deren inneren Abläufen – zumindest so weit, dass man einigermaßen beurteilen kann, was man gerade im Begriff ist zu tun.

In Bezug auf Phishing gibt es eine gute Nachricht: Eigentlich sind es gar nicht so viele Dinge, auf die man achten muss, um einigermaßen sicher durch – und eben nicht in – das Netz zu gehen.

Die Bedrohung

Bevor wir auf Angriffe und Gegenmaßnahmen eingehen, sei das Bedrohungsszenario skizziert, das als Phishing bezeichnet wird.

Als Ersatz für das persönliche Erscheinen im Geschäft, das eine Identität bildet, weist man sich beim digitalen Shopping in den meisten Fällen durch Nennung eines Namens (UserID, Kontoname, Nickname) und eines Geheimnisses (Passwort, PIN, Geheimzahl) aus.[5)] Wird die Kombination von Name und Geheimnis Dritten bekannt, können diese im Namen des Berechtigten alle Verfügungen treffen, die das System ermöglicht. Bei einem Bankkonto sind die Konsequenzen offensichtlich.

Es gibt eine ganze Reihe von Wegen, wie das vertrauliche Passwort in die falschen Hände geraten kann. Die meisten davon fallen in eine der beiden folgenden Kategorien:

- Der Geheimnisträger gibt es freiwillig preis[6)] oder

- der Bösewicht belauscht den Geheimnisträger, während dieser sich mit dem Passwort ausweist.

Eine Variation dieses Themas, wenn z.B. Einmalpasswörter, TANs oder zeitabhängige Passwörter verwendet werden:

- Der Bösewicht klinkt sich in die Kommunikation zwischen Geheimnisträger und System ein und verändert deren Inhalt.

Die scheinbar einfache (Techniker-)Antwort auf diese Probleme – *„Verwenden Sie doch HTTPS!“*[7)] – hat allerdings einen Haken: HTTPS hilft nicht, wenn der Benutzer nicht den Server seiner Bank, sondern den des Bösewichts kontaktiert. Ihn dazu zu überreden, genau darum geht es beim Phishing.

Panik killt gesunden Menschenverstand

Technik wird häufig als kinderfressendes Monster erlebt, vor dem man sich lieber fürchtet, als gelassen darüber nach-

---

2) siehe Artikel *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. www.univie.ac.at/comment/06-1/061_31.html

3) Seebach, Peter: *The Hacker FAQ* (www.plethora.net/~seebs/faqs/hacker.html)

4) Seebach, Peter: *The Manager FAQ* (www.plethora.net/~seebs/faqs/manager.html)

5) Chipkarten stellen bei der Mehrzahl der Anwendungsszenarios lediglich eine teilweise Verbesserung mit enttäuschendem Sicherheitsgewinn dar.

6) Dies ist ein Vorteil der Passwörter: Man kann erforderlichenfalls ein Recht befristet hergeben und gleich darauf durch Änderung des Passworts wieder zurücknehmen. Bei biometrischen Verfahren geht beides nicht.

7) siehe Artikel *WWW + SSL = HTTPS* auf Seite 46

8) Glücklicherweise handelt es sich hier noch um eine Simulation: Das Passwort-Formular versendet das eingegebene Passwort nicht, und der abgerufene Server befindet sich im Wohnzimmer des Autors. Obwohl die verlinkte Seite von einer Uni-Webseite optisch kaum zu unterscheiden ist, hat dieser „Phishing-Server“ – wie beim echten Phishing – netzwerktechnisch und administrativ nichts mit der Universität Wien zu tun.

zudenken. Angenommen, jemand würde folgende Nachricht massenweise an Uni-Mailadressen verschicken:

```
From: Sicherheit <password@univie.ac.at>
To: Uni-Angehoerige <password@univie.ac.at>
Subject: Diebstahl Ihres Passwortes

Sehr geehrte Damen und Herren,

Österreich ist derzeit von einer großangelegten
elektronischen Betrugswelle betroffen. Es mehren
sich die Berichte, dass in zahlreichen öffent-
lichen Einrichtungen die geheimen Nutzerkennungen
gestohlen worden sind. Damit können jetzt Unbe-
kannte Ihre eMail lesen, auf Ihre Dateien zu-
greifen, Ihre Homepage ändern, ein Diensthandy
bestellen, mittels CTI Ihr Telefon kontrollieren
und so weiter.

Wir ersuchen Sie dringend, Ihre Nutzerdaten auf
folgender Webseite zu prüfen:

http://security.univie.atat.at/validation.htm

Damit können wir sichergehen, dass Ihr Zugang
nicht missbraucht wurde. Wenn Sie nicht innerhalb
der nächsten Tage Ihren Zugang bestätigen, müssen
wir diesen leider deaktivieren.

Mit freundlichen Grüßen,
Ihre IT-Sicherheitsabteilung
```

Selbst wenn die Mehrheit unserer BenutzerInnen sich nicht ins Bockshorn jagen lässt: In der ersten Aufregung über die Gefahr eines massiven Eingriffs in die Privatsphäre würden wohl allzu viele sofort auf den angegebenen Link klicken. Dieser führt aber nicht zu einer Seite der Uni Wien (auch wenn die angezeigte Seite so aussieht), sondern zu einem Phishing-Server.[8)] Auf diese Weise könnten angesichts unserer nicht geringen Benutzerzahlen sicher einige tausend Mailbox- und Unet-Passwörter „gewonnen“ werden.

Was ist passiert? Der Geheimnisträger hat sich reinlegen lassen und selbst sein Geheimnis verraten. Dagegen sind keine technischen Maßnahmen möglich. Hilfreich, aber leider nur spärlich vorhanden, sind Schulungen und eindeutige Handlungsanleitungen.

Gute Ratschläge, kostenlos

Aus dem geschilderten Szenario lassen sich einige allgemeine Empfehlungen ableiten:

- Achten Sie bei sensiblen Transaktionen darauf, dass der URL der angezeigten Seite mit `https://` beginnt und dass das **Schloss-Symbol rechts unten im Browserfenster geschlossen**  ist (im Browser Firefox wird bei verschlüsselten Seiten zusätzlich die Adresszeile gelb hinterlegt). Lassen Sie sich nicht von Bildchen innerhalb einer Seite, die behaupten, diese sei sicher, in die Irre führen: Jeder HTML-Anfänger kann ein Logo in eine Webseite einblenden.

- Rufen Sie sensible Seiten soweit wie möglich über die **Bookmark-Funktion** Ihres Browsers auf (für den Urlaub können Sie diese auch als Webseite exportieren und auf Ihrer Homepage an geeigneter Stelle speichern). Dann kann Ihnen niemand plötzlich einen gefälschten URL unterjubeln.

- Prägen Sie sich wenigstens bei Ihrer Bank den **Domainnamen** ein und behalten Sie im Auge, wie deren URLs aussehen. Wenn diese nicht mehr wie gewohnt – z.B. mit `https://telebanking.meine-bank.at/` – beginnen (zu beachten sind `https`, der richtige Domainname und dass der Schrägstrich unmittelbar dahinter liegt), sondern stattdessen beispielsweise

  - `https://192.168.23.44/xxx`
    (also eine IP-Adresse),

  - `https://telebanking.meine-bank.at@eine.andere.domain/xxx`
    (also ein @-Zeichen vor dem Schrägstrich),

  - `https://telebanking.meine-bank.as/xxx`
    (also ein anderes Land) oder

  - `https://telebanking.maine-bank.at/xxx`
    (also eine geringfügig abweichende Schreibweise)

  erscheint, sind Sie höchstwahrscheinlich auf einer Phishing-Seite gelandet. Leider sind mehr Methoden der URL-Verschleierung bekannt, als hier aufgezählt werden können, aber häufig geben sich Phisher in dieser Hinsicht keine besondere Mühe.

- Wenn Sie den Verdacht haben, fehlgeleitet worden zu sein, kontrollieren Sie das **Zertifikat** (siehe Seite 50): Stimmen Name und Adresse? Ist der Aussteller vertrauenswürdig, ist die Zertifikatskette vollständig? Eine gute Idee ist es, das bereits frühzeitig an bekannten Seiten (z.B. `https://www.univie.ac.at/`) auszuprobieren.

- Vorsicht bei Links, die Sie **per eMail** erhalten haben! Diesem wichtigen Punkt widmet sich der folgende Abschnitt.

Gefahrenquelle eMail

Über die Probleme, die eMail als Virenträger und Belästigungsmedium mit sich bringt, wird seit Jahren in allen einschlägigen Medien ausführlichst berichtet. Die zahlreichen Täuschungsmöglichkeiten werden durch das fragwürdige Feature „formatierter“ HTML-Mails um eine Facette bereichert, die zum Missbrauch förmlich einlädt:

Wenn Sie in einer eMail einen Link auf `https://telebanking.meine-bank.at/xxx` sehen, bedeutet das noch lange nicht, dass Sie ein Klick darauf auch tatsächlich zur angegebenen Seite führt. Was bei Webseiten normal ist, nämlich dass sich der auf der Seite angezeigte Link-Text

ZID, fisch mit!

Unfreiwillige Mithilfe beim Phishing

Wer phishen geht, möchte dabei natürlich nicht erwischt werden. Daher verwenden Phisher nicht ihren eigenen Server, sondern missbrauchen fremde Rechner, zu denen sie irgendwie Zugang erhalten haben. Ist ein solcher gekaperter Rechner im Bereich des österreichischen Wissenschaftsnetzes ACOnet angebunden, sorgt das ACOnet-CERT (siehe Artikel *Kammerjäger im Netz* in *Comment 06/1*, Seite 31 bzw. unter `www.univie.ac.at/comment/06-1/061_31.html`) dafür, dass dieser Zustand schnellstmöglich behoben wird. In den meisten Fällen ist der Tathergang relativ unspektakulär: Mit Hilfe eines Virus (genauer: Trojaners) oder eines schwachen Passworts, das mittels automatisiertem Ausprobieren „erraten" wurde, bemächtigt sich der Phisher eines Rechners und missbraucht ihn – vom Anwender unbemerkt – als Webserver für Phishing-Seiten. Einmal jedoch war unser eigener Webserver WWW.UNIVIE.AC.AT auf ungewöhnliche Art und Weise daran beteiligt, Zugangsdaten einer südamerikanischen Bank zu erhaschen:

Was geschah?

Die Webseiten eines Instituts der Uni Wien enthielten eine Übung, in deren Rahmen ein Webformular auszufüllen war. Dabei wurde ein verbreitetes, vorgefertigtes CGI-Skript dazu verwendet, die in diesem Formular eingegebenen Daten automatisch per eMail an den Übungsleiter zu übermitteln. Dummerweise ist dieses Skript so gestaltet, dass es sämtliche Anweisungen – vor allem die eMail-Adresse, an welche die Daten zu senden sind – aus den ihm übergebenen Formulardaten nimmt. Unserem Phisher kam dieses Übungsskript gerade recht: Da es willig und ungeprüft beliebige Daten an beliebige Adressen sendet, spielte es ihm auf nur schwer nachzuvollziehende Weise die erschlichenen Bankcodes zu. Um es zusammenzufassen: Ein von einem Institut auf dessen Webseiten installiertes Skript zur Auswertung von Webformularen wurde von einem Phisher für seine Zwecke mitverwendet, und dazu musste dieser nicht einmal in den Uni-Webserver einbrechen.

Die Reaktion

Als die betroffene Bank das ACOnet-CERT kontaktierte, waren die Phishing-Webseiten, die auf den Uni-Webserver verwiesen hatten, bereits aus dem Netz genommen worden. Von Seiten des Instituts wurde das Skript zügig entfernt. Die Logfiles des Webservers verzeichnen auch den sogenannten *Referer*, das ist die Seite, von welcher der Besucher auf den Server verwiesen wurde. Daraus ergab sich, dass das missbrauchte Skript an diesem Tag nur von Phishing-Opfern aufgerufen worden war. Um der Bank die Chance zu geben, die Kunden, die auf den Phishzug hereingefallen waren, zu identifizieren und zu warnen, wurden ihr etwa 250 betroffene IP-Adressen übermittelt.

Spurensuche

Leider war nicht mehr feststellbar, wohin die Formulardaten gesendet wurden: Da die Phishing-Webseiten bereits entfernt worden waren, konnten wir den Vorgang nicht mehr „live" beobachten. Das Skript selbst führt keine Protokolle und verwendete für den Versand keine uns bekannten Mailserver, deren Logfiles uns Hinweise hätten geben können.

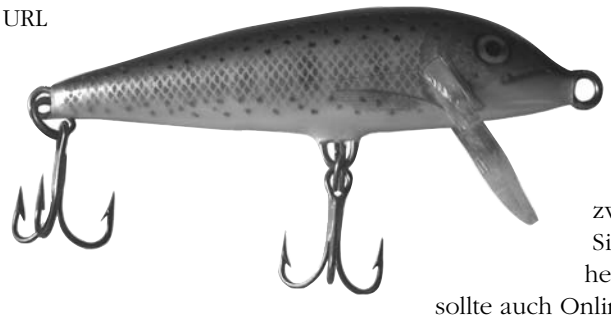
Eine weitere Frage beschäftigte uns: Wie kam ein offenbar im spanischen Sprachraum agierender Phisher darauf, dass es tief vergraben in den Webseiten eines österreichischen Universitätsinstituts ein Skript namens `uebung.cgi` gibt, das sich gut gebrauchen lässt? Ein Blick auf den Referer, der beim ersten Zugriff auf dieses Skript im fraglichen Zeitraum aufgezeichnet worden war, beantwortete diese Frage (Daten leicht verändert):

```
10.14.60.123 - - [16/Mar/2006:02:45:48 +0100] "GET /Institut/Lehre/uebung.cgi HTTP/1.1"
200 47 "http://www.google.es/search?hl=es&q=inurl%3A.cgi+intitle%3ANo+input+data&meta="
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
```

Des Rätsels Lösung: Der Robot von Google gibt beim Indizieren des fraglichen Skripts natürlich keine Formulardaten ein. Das führt zur Fehlermeldung *No input data*, und diese wird von Google gespeichert. Genau danach – das ist im Referer zu lesen, da bei Google die Frage immer Teil des URLs ist – hat der Phisher gesucht und auf diese Weise zu uns gefunden. Die gezeigte Abfrage wurde also vom Phisher selbst getätigt; folglich hätte `10.14.60.123` seine IP-Adresse sein müssen. Leider führte auch diese Spur nicht zum Täter: Es handelte sich um einen trojanisierten PC, der als Proxy missbraucht wurde. Naturgemäß war nicht mehr festzustellen, von woher der Phisher auf diesen PC zugegriffen hatte.

Eine Konsequenz konnten wir aus dem Ereignis ziehen: Wir befragen jetzt selbst regelmäßig Google, um solche verwundbaren Skripts in unserem Netz aufzuspüren und deren Betreiber rechtzeitig warnen zu können.

und der tatsächlich verlinkte URL unterscheiden, kann in eMails gewinnbringend verwendet werden: Gezeigt wird der richtige URL der Bank, verwiesen wird hingegen auf die Phishing-Seite.



Die notwendigen Vorsichtsmaßnahmen sind also eigentlich ganz einfach:

- **Links, die Sie per Mail erhalten haben, sollten Sie möglichst überhaupt nicht anklicken.** Besonders wenn es sich um ein Service handelt, für das Sie ein Passwort oder dergleichen besitzen, ist es besser, dessen Homepage aus den Bookmarks heraus aufzurufen und zu versuchen, mittels „Durchklicken" zur angegebenen Seite zu gelangen.

- Je dringlicher die Nachricht ist und je größer die geschilderte Katastrophe: **Überprüfen Sie, z.B. durch Anruf bei der Hotline, ob die Story echt ist.** Die Telefonnummer dürfen Sie natürlich nicht der eMail entnehmen – es könnte ja auch die gesamte Hotline ein Fake sein.

- Wenn Sie meinen, dass Sie dem Absender vertrauen können, und einen Link daher doch anklicken wollen, sollten Sie folgende Punkte beherzigen:

  - **Geben Sie keine Passwörter oder sonstigen vertraulichen Daten auf per eMail-Link erreichten Seiten ein.**

  - **Kontrollieren Sie auf jeden Fall das TLS/SSL-Zertifikat**, wie auf Seite 50 beschrieben.

  - **Prüfen Sie, sofern vorhanden und möglich, die digitale Unterschrift.** (Es ist sehr bedauerlich, dass sich diese Technik in eMail bisher nicht durchgesetzt hat, daher wird das leider nur selten gelingen.)

  - **Bedenken Sie, dass Sie der Absender unwissentlich auf eine Phishing-Seite verweisen könnte**, der er selbst soeben auf den Leim gegangen ist.

Es gibt viel zu tun

Geschäfte im Internet lassen sich auch für NichtexpertInnen sicher – also mit vertretbarem Restrisiko – gestalten. Wenn die Betreiber von Telebanking-Seiten, Online-Shops usw. mitarbeiten und ihrerseits eine klare Anti-Phishing-Strategie festlegen, dann könnten die obigen Ratschläge noch um einiges kürzer ausfallen.

Banken und andere Betreiber heikler Services müssen einen Mittelweg zwischen Benutzerfreundlichkeit und Sicherheit finden. So wie das Sicherheitsballett in Flugzeugen Vorschrift ist, sollte auch Online-KundInnen eine Anleitung gegeben werden, die z.B. folgenden Inhalt haben könnte:

```
Das Team der Firma WirSindToll freut sich, Sie als Kunde in unserem Online-Shop begrüßen zu können. Wir setzen stets die allerneuesten Sicherheits-Technologien ein. Damit diese zum Tragen kommen, beachten Sie bitte vier einfache Tipps:

• Rufen Sie unseren Online-Shop stets nur aus den Bookmarks Ihres Browsers auf, nicht durch Links in eMails oder fremden Webseiten.

• Wenn Sie bei uns einkaufen, achten Sie darauf, dass der URL im Browserfenster immer mit https://shop.wirsindtoll.at/ beginnt.

• Achten Sie darauf, dass das Schloss rechts unten im Browserfenster geschlossen ist.

• Niemals senden wir Ihnen eMail, die einen anzuklickenden Link enthält und zur Aufforderung führt, ein Passwort einzugeben. Wenn Sie eine solche eMail-Nachricht erhalten, löschen Sie diese ganz einfach.
```

Vergleichen Sie diesen Text mit den Unterlagen Ihres Telebanking-Zugangs. Vermutlich werden Sie enttäuscht feststellen, dass dort nur zu lesen ist, dass wegen toller Verschüsselung alles ganz sicher ist und Sie sich keine Sorgen machen müssen. Diese Banken haben ihre Hausaufgaben leider nicht gemacht – wohl, um die Kunden nicht zu verunsichern. Hier hätte die Chefetage besser ihren TechnikerInnen zugehört, denn ein falsches Gefühl der Sicherheit zu erzeugen, ist natürlich der Kardinalfehler schlechthin.

Phishing ist ein Phänomen mit furchterregendem Entwicklungspotential. Zum einen gilt es daher, durch technische Mittel, Aufklärung und zweckmäßige Sicherheitsgebräuche auf Betreiberseite dagegen vorzugehen.[9] Zum anderen zeigt sich wieder, dass mit Viren, Würmern oder Trojanern infizierte PCs ein unkalkulierbares – aber jedenfalls gewaltiges – Sicherheitsrisiko darstellen und dass Softwarehersteller, Netzbetreiber und AnwenderInnen gemeinsam alle erdenklichen Anstrengungen unternehmen müssen, um die zahllosen verseuchten Rechner aus dem Verkehr zu ziehen.

Alexander Talos ■

9) Auch die Uni Wien ist in dieser Hinsicht noch kein leuchtendes Vorbild, aber wir arbeiten daran. Dass es bei uns noch niemand ernsthaft probiert hat, hat wohl zwei Gründe: Noch ist die Phishing-Branche in Europa nicht so richtig in Fahrt gekommen, und wir sind für Phisher nicht so interessant wie eine Bank.