

# Unauthorised access (hacking)

I have a problem with unauthorised access; what should I do?

## Introduction

There is a misconception that “hacking” - unauthorised access to data through the compromising of computer security - is not as common a problem in Ireland as it is in other countries. It is true that the possibility of skilled hackers breaking into a network from outside never represented as serious a threat to the security of data held on computer systems as was some times made out. What has often been forgotten, however, was that the threat of hacking by insiders to organisations was always far more serious, and the potential for damage to organisations today from this threat is, if anything, higher today than it ever was in the past.

Ideally any organisation should have some kind of incident response plan to deal with hacking incidents but most, we find, do not. We have prepared the following brief document for IT personnel or other managers who are faced with an unauthorised access incident or are thinking of preparing a plan for dealing with it. This document is not a complete incident response plan. We hope, however, that it will provide a useful guide to the key issues in dealing with a hacking incident, and may help anyone faced suddenly with dealing with such an event. We think it deals with most of the main issues facing organisations experiencing problems of this nature.

Grant Thornton has extensive experience helping organisations deal with crises such as these. We have helped many others prepare detailed incident response plans to allow them to quickly react to, control and resolve incidents that threaten to disrupt or damage their organisations. If you need more advice, or would like to talk to us about our services, we would be delighted for you to get in contact with us.

## Internal and external hacking

Computer security specialists normally distinguish between internal and external network attacks. This is because intruder profiles, methods of attack and intruder objectives can vary significantly between internal and external attacks.

### External attacks

Attacks where the intruder has no privileges on the target network, and either gains access from outside the network perimeter (usually the firewall), or by evading or undermining the target's physical and/or network security measures to achieve some degree of access to the target's internal network.

### Internal attacks

Attacks where the intruder has legitimate privileges on the target network. Access is obtained using existing privileges, privileges the intruder has extended without permission, or privileges stolen from other users. The objective of the intrusion is to gain access to data and resources to which the intruder is not authorised.

External attacks can be made against the internal network, using the target's own computers. This is often done with the active or passive collusion of the members of the target's own staff. However, if the ultimate initiator of the attacks is someone holding no legitimate privileges on the network, then it is considered an external attack.

Internal attacks are typically far more common than external ones.

### Modes of external attack

The principal mode of external hacking seen in Ireland is based on simple credential theft, i.e. stealing or guessing another user's password and using it to gain access, but there are many other ways of compromising a computer network from the outside:

#### External attack vectors

- **access through weak, stolen or lost credentials.** The most common form of attack.
- **access through malware infection.** Another common mode of attack. An insider activates a "Trojan Horse" program, intentionally or unintentionally, that opens access to their network.
- **access through compromise of remote access systems.** Making use of the target's own remote access connections.
- **compromised third-party access.** Instead of hacking the target, the attacker hacks an individual or organisation known to have access to the target's systems.
- **access through physical penetration.** Gaining access to computer networks by actually entering the target's premises
- **access through modem dial-up.** Some organisations still maintain dial-in connections for legacy systems. These can be very insecure.
- **unauthorised access with co-operation of the organisation's staff.** By threatening or subverting members of staff or placing confederates on the staff of the target organisation.
- **access through wireless systems.** Wireless (WiFi) connections are particularly problematic as they can be difficult to set up securely, can be cheaply set up on networks by users without the knowledge of IT staff and if compromised can provide direct access to internal systems, bypassing network perimeter security.
- **direct penetration through perimeter systems.** Perhaps the most difficult and least common approach

### Modes of internal attack

Internal attacks are considerably more common than external ones. "Insiders" already have credentials and privileges on the target network, and have direct access to systems computers inside the network's secure perimeter. Insiders usually have more time and opportunity to discover how to gain access to restricted systems and directories. They are also more likely to know which computers contain the material of most value to them:

#### Common sources of internal attack

- **unauthorised access by IT personnel.** In Irish organisations a disproportionate amount of unauthorised access is carried out by members of the IT staff, largely because they are most likely to have high-level computer security privileges.
- **unauthorised access by non-IT staff with high-level privileges.** Non-IT users should not, generally, have high-level network security privileges, but we occasionally find cases where this has happened. In other cases we have seen non-IT users obtain these privileges through hacking, persuasion, bribery, threats or outright theft.
- **access through theft of other users' credentials.** Some ordinary users are given access to systems restricted to others. It is not uncommon to find such credentials stolen from their holders, or even voluntarily shared by them.
- **access to inadequately secured systems.** Some sensitive systems are simply not given sufficient protection, and can be straightforwardly compromised by intruders without high level privileges.

### Hacking telltales

Perhaps the biggest problem with dealing with a hacking incident is determining whether or not you have been hacked in the first place. Implementing security technologies such as intrusion detection and intrusion prevention systems can help. However, there are a number of other key indications that might reveal the presence of a hacker.

### Indicators of unauthorised access

- **unexplained system failures (“crashes”)**. Some attacks can destabilise computer systems and networks. If one or more systems start behaving erratically it may be a sign that hacking exploits are being run on them.
- **unexplained access to users’ e-mail accounts**. Caused by hackers searching for valuable information.
- **unexplained modifications to users’ personal file storage**. Caused by hackers searching for useful data.
- **suspicious browsing**. e.g. an administrative user accessing file after file on many user accounts.
- **unauthorised system access requests**. Often indicate stolen user credentials.
- **Anomalies**. Such as a sudden deterioration in performance, corruption of data or new windows unexpectedly popping up.
- **unauthorised new user accounts**. Indicating compromise of administration privileges
- **activity on system or dormant user accounts**. indicating theft or compromise of account credentials
- **repeated lock-outs in a single user account/increase in helpdesk password change requests**. May indicate password guessing attempts
- **probe activity** (e.g. multiple unsuccessful login attempts from another computer). This is a reliable indication of attempted intrusion.
- **new files in system directories**. Usually with unusual file names, can be hackers’ toolkit (“rootkit”) components.
- **alterations to log files**. If the application and system logs on a windows computer are corrupt it indicates that an attempt has been made to change the log files.
- **unexpected data modification or deletion**. Can indicate sabotage or intrusion.
- **anti-virus/anti-malware alerts on multiple computers**. Can be caused by the presence of hacking tools.
- **changes in file characteristics or dates**.
- **deviation from normal network traffic flows**. Can be indicative of an attacker scanning the network.
- **unexplained, poor system performance**. Potentially caused by scanners or parallel user sessions.
- **use of non-standard communications protocols** such as Internet Relay Chat (IRC), Internet News Group Protocol (INP), Trivial File Transfer Protocol (TFTP) or unauthorised encrypted protocols.

### Basic incident response

#### Validating the incident

It is often difficult to quickly confirm whether or not a hacking attack is under way. It is probably safer to err on the side of caution when deciding whether or not to initiate counter-intrusion measures. There are some places where useful information can be found that may make it easier to come to a decision:

### Sources of validation information

- **event logs**. The event logs, particularly the security log, are perhaps the most important tool in investigating hacking attacks.
- **file system analysis**. Activity by hackers will change the time and date stamps of files in various directories of affected computer. If gateway or file storage systems are affected this way it may indicate an attack.
- **firewall, router and intrusion detection systems**. Hackers usually have to probe for weaknesses on other computers. This software activity will be recorded in the logs of certain system devices.
- **Antivirus/Anti-spyware software**. Antivirus software is capable of detecting the hacking tools and exploits used by hackers.
- **file integrity checking systems**. File integrity systems, such as Tripwire, detect changes to key files on the systems where they are installed. An alert on such a system is a very strong indicator that an attack is under way. Of course, these systems have to be installed in the first place.
- **understand normal behaviour**. In order to know if something is unusual, you must first understand what “usual” is. Try to establish clearly what exactly is different.
- **maintain a knowledge base**. Keep a database of information that can be quickly referenced in event of an attack. It can be as simple as a list of security websites, the phone numbers of incident response specialists (ours can be found at the end of this guide), and the locations of key log files.
- **information from other sources**. Investigators need not only rely on technical evidence. Ordinary computer users may notice that something is wrong before anyone else.

## Priorities

### External attacks

Your priorities in dealing with hacking attempts depend on whether or not the intrusion comes from inside or outside the organisation. With external attacks it is often very difficult to take legal action against an intruder, so the priority must be as follows:

#### External intrusion - containment/eradication

- identify and secure affected systems - if necessary by powering systems down;
- identify the point of intrusion and close it off - if necessary by powering systems down;
- sweep affected systems for backdoor software or rootkits. If you are not certain all have been cleared consider restoring affected systems from backups;
- preserve all key log files on computers, firewalls and other network devices. Grant Thornton's guide to preserving evidence can be found on our IT forensics website;
- change all passwords and other credentials - prioritising administrative and high-privilege accounts, including those assigned to services such as the backup system;
- replace all certificates;
- check security patch status of all systems and patch all deficient computers to current; and
- assess the extent of data compromise and loss.

Note that, while computer forensic evidence should be preserved if possible, securing systems is a higher priority. The likelihood of successful prosecution is low where an attack has originated from outside the network.

## Priorities

### Internal attacks

Internal attacks are more difficult to control, as the intruder cannot be shut out of the network perimeter, and may be in possession of legitimate network privileges. In this case it will take longer to contain and eradicate the incident. It will also be necessary to pursue and possibly prosecute the intruder, so the preservation of forensic material is more important.

#### Internal intrusion - containment/eradication

- identify and secure affected systems - if necessary by powering systems down or isolating systems;
- disable any user accounts suspected of hacking, or of having been compromised;
- create computer forensic images of key affected systems. These will be necessary to identify the source of any internal intrusion and to take legal action afterwards;
- preserve all key log files on computers, firewalls and other network devices. Grant Thornton's guide to preserving evidence can be found on our IT forensics web-site;
- enhance physical security measures. Ensure no trespassers are present on organisation premises;
- sweep affected systems for backdoor software or rootkits. If you are not certain all have been cleared consider restoring affected systems from backups;
- change all passwords and other credentials - prioritising administrative and high-privilege accounts, including those assigned to services such as the backup system;
- replace all certificates;
- check security patch status of all systems and patch all deficient computers to current; and
- assess the extent of data compromise and loss.

## Other issues you may need to consider

**Documentation:** As with any incident, the first responder should document all significant events, observations and actions taken from when the incident is first detected. If these are not recorded immediately it is very likely that key details will be missed which may delay or reduce the effectiveness of later remedial actions.

**Reporting:** Managers and key affected stakeholders should be advised of the event:

#### Consider advising:

- General management;
- IT management;
- Business/Operational Unit Management;
- Legal;
- HR/Industrial Relations;
- Public Relations; and
- Internal Audit/ Fraud Control.

## Remediation and reporting

### Remediation

Remediation involves putting measures in place to ensure, as far as possible, similar incidents do not reoccur. In the case of virus and other malware infections we suggest the following precautions, if they are not already in place:

#### Remediation actions

- develop a full incident response plan for future intrusions, based on the lesson learned from the incident just finished. Grant Thornton can help you develop an effective plan. Our contact details are below;
- anti-virus software should be updated daily;
- consider installing file integrity systems on key systems, particularly those on the network perimeter;
- prohibit the use unauthorised software on your computer systems;
- keep your computers and other systems up to date with application and operating system patches;
- introduce a policy of "least-privilege" across your network. If possible, applications should be set-up to run without high level privileges. These precautions will lessen hackers' ability to make use of high level user accounts;
- teach your staff out to devise and remember complex passwords. Explain to them the importance of proper password procedures;
- ensure that only complex passwords are used on your network, and that all passwords are changed regularly. Note, however, that if passwords are complex it is not necessary to change them as often;
- use Wireless technology with great care. Perform regular sweeps to identify rogue wireless connections on your network Treat any legitimate wireless subnet as a "semi trusted" or DMZ network. Never directly connect core servers to wireless-equipped sub-nets;
- perform regular scans of both internal and external systems to look for likely points of intrusion; and
- consider engaging outside consultants to perform a penetration test of your network.

### Reporting

It is often necessary to prepare a formal report on any incident for senior managers, regulators or other stakeholders. In writing the report on the incident it is probably worthwhile considering the following issues:

#### Possible report content

- the source of the breach (if determined);
- contributory factors to the incident;
- timeline of incident response activities;
- actions taken to recover from the incident;
- assessment of any damages incurred, data lost;
- further remedial actions required; and
- other relevant information.

### If you need more advice

Our incident response and computer forensics specialists have helped hundreds of organisations deal with incidents quickly and effectively, helping them resolve their problems with the minimum of loss, disruption or distress.

If you would like to talk to us about computer forensics, incident response planning or any other issue, please feel free to give us a call at the numbers below.

### Contact

**Paul Jacobs**

Partner, Forensic & Investigation Services  
D +353 (0)1 6805 835  
E [paul.jacobs@grantthornton.ie](mailto:paul.jacobs@grantthornton.ie)

**Andrew Harbison**

Director, IT Forensics & Investigation Services  
D +353 (0)1 6805 766  
M +353 (0)86 040 7211  
E [andrew.harbison@grantthornton.ie](mailto:andrew.harbison@grantthornton.ie)

W [www.grantthornton.ie/computerforensics](http://www.grantthornton.ie/computerforensics)

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should always be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. Grant Thornton is authorised by the Institute of Chartered Accountants in Ireland to carry on investment business.

