THE BOLLINGER LAW FIRM, LLC
104 Rock Rose Lane, Radnor, PA 19087
610-688-6883

Protect Against Hacking Techniques

Malicious hackers penetrate computers, devices, and objects by using malware designed to steal information, or damage systems, networks and software, or take over computers, devices or objects, or "just look around." No matter by what means, the harm to information, communication, and technology is powerful and severe at countless levels.

Below are examples of some current hacking techniques, descriptions of some of the techniques, examples of how to prevent some of the hacking, and finally, examples of what to do if hacking happens. They are applicable whether with mobile devices, computers, or other "things" connected to the Internet, such as wearables, medical devices and other objects.

Examples of Hacking Techniques

- Keylogging
- Phishing
- Brute force attack
- Social engineering
- Rootkit
- Trojan horse
- Virus
- Worm
- Retrieving "deleted" data from poorly sanitized media
- Broken authentication and session management attacks
- Ransomware
- DDoS
- Injection attacks
- Cross site scripting attacks
- Password cracking
- Traffic Sniffing
- IP spoofing
- Blue snarfing
- Malvertizing
- Cookie theft
- DNS cache hacking
- Vehicle hacking
- Hacking of other "smart" devices
- And, others

About the Hacking Techniques

1. Keylogging	In a keylogger attack, attackers use software to track all of the user's keystrokes. By doing so, they can capture login information. *To Prevent*: Install anti-malware software to detect if a keylogger is installed. Use network monitors to be alerted if someone tries to connect to the network. Use one-time passwords or passphrases. *If It Happens:* Update your anti-malware software and run the anti-malware software to remove the keylogger. If the anti-malware software cannot remove the keylogger successfully, seek technical assistance.

2. Phishing	In a phishing attack, the attacker impersonates a legitimate business in order to gain access to a user's account. It is often in the form of an email that appears to be sent by the target's package delivery from FedEx or UPS, or order confirmations from online stores, or banks. *To Prevent*: Be suspicious of emails from unrecognized senders that ask for confirmation of personal information or try to make threatening or urgent requests. Do not give personal information over unsecured and unknown websites, or over the phone. Use anti-malware tools on individual computers. Organizations can use a Secure Email Gateway to scan content and more effectively filter email. *If It Happens*: Contact credit agencies, law enforcement, and employers. Change passwords; update and scan with anti-malware software and install software updates.
3. Brute-force attack	In a brute-force attack, the attacker uses a trial-and-error method to determine a pin or password. *To Prevent*: Ensure that the system is configured to render the system unusable for a short period of time after an incorrect password or passphrase is used; use strong passwords or passphrases that include special characters and are easy to remember but hard to guess. *If It Happens*: If the credentials were breached, change account names and passwords immediately; figure out what information was affected then do damage control; contact credit agencies to place alerts on accounts.
4. Traffic sniffing	A traffic sniffer can be used to intercept and log the traffic that passes over a digital network. While this can be used for law enforcement purposes, it can also be used by criminals. *To Prevent*: Use end-to-end encryption for all transmissions. Examples include HTTPS, SFTP, and SSH, and VPN. *If It Happens*: Take steps to implement end-to-end encryption of your data, especially login information.
5. Rootkits	A rootkit is software that is designed to allow privileged access to areas of a system that otherwise would not be accessible. This could provide the attacker with total control over the system. *To Prevent*: Be very vigilant when opening email attachments and other files; install anti-malware software. *If It Happens*: Update and use the anti-malware software to try and remove the rootkit. If anti-malware software cannot remove the rootkit, it may be necessary to erase the computer.

6. Ransomware	This software can block access to a system. The attacker refuses to remove the block until a ransom is paid. *To Prevent*: Back up the system regularly; install anti-malware software and regularly update systems with current patches. *If It Happens*: Remove the impacted system from the network and turn it off; call a trusted source for help and remove the ransomware while offline. If you have a backup, restore data from backup.
7. Injection attacks	Attackers provide specially crafted input data into the SQL (language used to communicate with a database) interpreter and trick the interpreter into executing unintentional commands. *To Prevent*: Adopt input validation techniques in which the user input is authenticated against a set of defined rules for strength, type, and syntax and also against business rules. Ensure that users with authorization to access the database have the least amount of privileges. Create application-specific database user accounts. *If It Happens*: Parameterize SQL queries; encrypting database tables and restricting access to a database server are valid security measures but building an application to withstand SQL Injection attacks is a crucial web application defense strategy.
8. Bluesnarfing	Hackers gain access to the data on a Bluetooth enabled device using the wireless technology Bluetooth. *To Prevent*: Set Bluetooth devices to “hidden” instead of discoverable; turn off Bluetooth when not using the capability; update software regularly for patches. *If It Happens*: Disable your phone, tablet, or laptop from Bluetooth and the internet.
9. Malvertising	Software that downloads or installs unwanted software through advertising platforms on the internet. *To Prevent:* Update browsers regularly and install anti-malware software. Disable Flash and Java if not needed. *If It Happens*: Run your anti-malware software to detect malware; remove any malware and revert to pre-virus backup.

10. Broken authentication and session management attacks	Authentication systems involve passwords, key management, session IDs, and cookies that allow a hacker to access your account from any computer (as long as they are valid). If a hacker exploits the authentication and session management system, they can assume that user's identity. *To Prevent*: Follow software development best practices and periodically check old application against current security best practices, such as the Open Web Application Security Project (OWASP) Top 10.[1] *If It Happens*: Change credentials and avoid using the affected software until a fix is developed.
11. Cross-site scripting	Attacks, also known as XSS attacks, occur when an application, URL "get request," or file packet is sent to the web browser window but bypasses the validation process. Once an XSS script is triggered, it's deceptive property makes users believe that the compromised page of a specific website is legitimate. *To Prevent*: Follow industry best practices in developing web-based software. For example, follow OWASP's SQL Injection Prevention Cheat Sheet.[2] *If It Happens*: Shut down any afflicted web-based applications and implement a fix.

Although it is challenging to keep pace with hackers' complicated disruptive techniques it is essential to stay apprised of their practices and take preventative action.

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[2] https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.md