DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

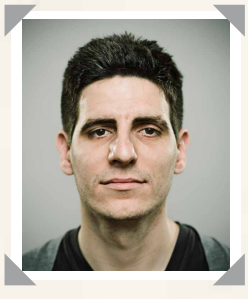
DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

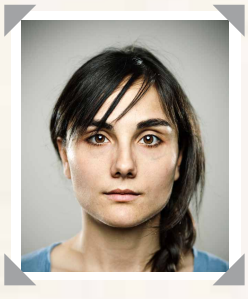
Glossar zum Thema Identitätsdiebstahl

TÄTER:
Tobi Taschendieb/ Andrea Ablenker

VERBRECHEN:
Diebstahl

GESUCHT WEGEN:
Taschendiebstahl





ALIAS:
Tobi, Die Tasche

BESONDERE KENNZEICHEN:
Kleine Narben an der Stirn, verursacht durch die Handtasche eines Opfers

ALIAS:
Andrea Klebefinger

BESONDERE KENNZEICHEN:
Tattoo von Einkaufstaschen am rechten Handgelenk

Dieses Duo stiehlt ganz klassisch Geldbörsen und Mobiltelefone aus Jacken-, Hosen- und Handtaschen – häufig sogar am hellichten Tag. Sie bevorzugen die Drängeleien durch Menschenmassen bei Sportereignissen und Konzerten.

Sie arbeiten im Team. Dabei sorgt Andrea für die Ablenkung, indem sie eine Einkaufstasche fallen lässt, um Hilfe ruft oder plötzlich vor Ihnen stehen bleibt. In diesem Moment rempelt Tobi Sie an, hält sich – scheinbar harmlos – an Ihnen fest und greift in Ihre Tasche.

Beliebte Tatorte sind auch U-Bahn-Stationen und Flughäfen. Sie verdecken ihre Hände mit einer Zeitschrift und suchen nach Menschen, die abgelenkt sind oder gerade telefonieren. Auf diese Weise stehlen sie häufig mehrere Geldbörsen innerhalb kurzer Zeit.

Sie stehlen auch Mobiltelefone und PDAs (Personal Digital Assistants), da diese Geräte häufig wertvolle persönlichen Informationen enthalten und selten mit einem Kennwort gesichert sind.

Achten Sie immer auf Ihre nähere Umgebung. Für Ihren Schutz können Sie Folgendes tun:

- Bewahren Sie Ihre Brieftasche in Ihrer vorderen Hosentasche auf, schließen Sie Ihre Handtasche, und tragen Sie sie vor sich (Diebe könnten den Trageriemen durchschneiden).
- Tragen Sie Ihre Geldbörse nicht in der Gesäßtasche oder im Rucksack, und legen Sie für Ihren PDA und/oder Ihr Mobilgerät ein Kennwort fest.
- Führen Sie nur dann Kredit- und EC-Karten mit sich, wenn Sie sie benötigen.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Trojaner Seabiscuit

VERBRECHEN:
Gaunereien

GESUCHT WEGEN:
Verwendung von Trojanern

ALIAS:
E-Mail-Reiter, Jockey

BESONDERE KENNZEICHEN:
Hufabdruck an der rechten Wade

Bei einem Namen wie Trojaner denken Sie möglicherweise zuerst an einen Kämpfer für das Gute. Aber Vorsicht: Denken Sie an die griechische Mythologie!

Trojaner ist in Wirklichkeit ein Heuchler und Lügner und gleichermaßen heißer Kandidat für „Beliebtester Nachbar" und „Intrigantester Nachbar". Ursprünglich versendete er E-Mails, die als Anlagen böswillige Dateien mitbrachten. Heute fügt er seine Payloads in kostenlose Fotos, PDF-Dateien und andere aus dem Internet herunterladbare Dateien ein.

Sobald er sich in Ihr System geschlichen hat, stehen ihm verschiedene Tricks zur Verfügung: Er kann Ihren Computer fernsteuern, persönliche Informationen, Dateien und Kennwörter hochladen sowie Keylogger und andere Tools herunterladen.

Er ist Champion des ultimativen Identitätsdiebstahl-Derbys der Phisher, Hacker, Botmaster und Keylogger, die weltweit mehr als 17 Mrd. € erbeutet haben.

Achten Sie darauf, sich mit den richtigen Maßnahmen zu schützen. Für Ihren Schutz können Sie Folgendes tun:

- Setzen Sie eine umfassende Sicherheits-Software ein, die sich automatisch aktualisiert.
- Drücken Sie die ESC-Taste, und machen Sie sich aus dem Staub, wenn eine Webseite behauptet, dass Sie eine Adobe Flash-Aktualisierung oder andere Downloads benötigen.
- Rufen Sie die Webseite des Herstellers auf, wenn Sie eine Aktualisierung herunterladen möchten. Verwenden Sie keine Download-Dateien von Drittanbieterseiten.

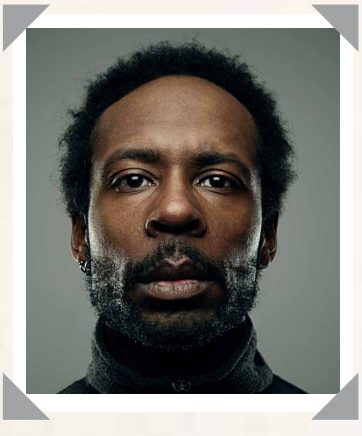
DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Tom „Der Skimmer“ McKohle

VERBRECHEN:
Kredit-/EC-Kartenbetrug

GESUCHT WEGEN:
Manipulation von Geldautomaten



ALIAS:
Absahner, Abgraser, Automatenkiller

BESONDERE KENNZEICHEN:
Freebird-Tattoo an der Wade

Tom „Der Skimmer“ McKohle ist nicht für seine Raffinesse bekannt, er ist aber auf jeden Fall technisch begabt. Der gewiefte Betrüger installiert spezielle Auslesegeräte (Skimming-Geräte) und kleine Kameras, die Ihre Kontoinformationen sowie Ihre Karten-PIN erfassen.

Wenn Sie einen der von ihm „getunten“ Bankautomaten benutzen, erfasst und speichert er Ihre Kartennummer und die PIN und verkauft sie an den Meistbietenden.

Ganz nach dem Motto „Wenn, dann richtig“ bevorzugt er große Gruppen seiner Opfer, damit er schnell reich werden und schnell wieder verschwinden kann.

Geldautomaten in der Nähe von Konzerthallen, Stadien, Tankstellen und kleinen Geschäften sind für ihn besonders interessant. Das Sammeln Ihrer Daten, die er zum Leeren Ihres Kontos benötigt, ist für ihn sehr schnell und bequem erledigt. Und für Sie kann es sehr teuer werden.

Es ist immer schwerer, Skimming-Geräte als solche zu erkennen. Für Ihren Schutz können Sie Folgendes tun:

- Verwenden Sie keine Bankautomaten, bei denen über dem Kartenschlitz oder Tastenfeld etwas aufgesetzt ist, oder die irgendwo klappern.
- Verwenden Sie möglichst immer den gleichen Geldautomaten.
- Decken Sie immer Ihre Hand ab, wenn Sie Ihre PIN eingeben.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Müllsucher-Daniel

VERBRECHEN:
Identitätsdiebstahl

GESUCHT WEGEN:
Wühlen im Abfall

ALIAS:
Müll-Man, Puzzle-Meister, Abfall-Rätsler

BESONDERE KENNZEICHEN:
Narben an Armen und Beinen vom Herumklettern in Müllcontainern

Daniel bezeichnet sich gern als Mitarbeiter der Stadtreinigung. In Wirklichkeit wühlt er sich durch den Abfall und verwandelt ihn in bares Geld.

Daniel durchsucht Müllcontainer nach Kontoauszügen, Anmeldebögen für Kreditkarten, Quittungen und anderen persönlichen Informationen, um sie in seine schmutzigen Finger zu bekommen.

Anschließend sucht er sich ein ruhiges Plätzchen und setzt die zerrissenen Dokumente wieder zusammen, damit er Ihre Identität stehlen, Ihre Kreditkartendaten missbrauchen und Ihnen Dreck anhängen kann. Wenn er sich ein vollständiges Bild von Ihnen machen will, sucht er nach Informationen, die Sie im Internet von sich preisgeben.

Oder er nutzt die im Abfall gefundenen Schätze, um Ihre Online-Kennwörter zu erraten. Und dann macht er sich auf den Weg zur Bank. Zu Ihrer Bank.

Sie merken meist zu spät, wenn ein Müllsucher an Ihre Informationen gelangt ist. Für Ihren Schutz können Sie Folgendes tun:

- Kaufen Sie sich einen guten Dokumentenschredder – und nutzen Sie ihn!
- Schreddern Sie alles, was persönliche Informationen enthält. Dazu gehören Geburtsdatum, Kreditkartennummer, Nebenkosten- und Telefonrechnungen, Personalausweis- und Führerscheinnummer sowie Quittungen.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Spionin Silberfuchs

VERBRECHEN:
Diebstahl persönlicher Daten

GESUCHT WEGEN:
Drahtlos-Sniffing

ALIAS:
Die Betrügerin, Fuchs-AG

BESONDERE KENNZEICHEN:
Fuchs-Tattoo am Fußknöchel

Silberfuchs handelt immer ganz schnell und kann auf eine umfangreiche Sammlung modischer Tools zurückgreifen. Sie liebt die Beute und den Tratsch, den sie im gemütlichen Internet-Café aufschnappt.

Sie gibt sich gern als kostenloser Wi-Fi-Hotspot aus und gewährt Ihnen Internetzugang über ihren Laptop. Dabei schnüffelt Sie nebenher Ihre Konto- und Anmeldedaten sowie andere persönliche Informationen aus. Mithilfe Ihrer Kennwörter kann sie sich bei Ihrem Konto anmelden, während Sie neben ihr sitzen und einen Cappuccino genießen.

Wenn Sie zudem die Dateifreigabe aktiviert haben, kann sie sich auf Ihrem Computer umsehen, Steuerformulare und Adressbücher kopieren oder Schad-Software installieren, die sie dann später steuern kann, wenn Sie bereits zuhause sind (siehe Keylogger und Trojaner).

Seien Sie ganz besonders vorsichtig, wenn Sie eine ungesicherte Drahtlosverbindung verwenden. Für Ihren Schutz können Sie Folgendes tun:

- Wählen Sie keine generischen oder Computer-zu-Computer-Netzwerke wie „Linksys“ oder „Kostenloses Wi-Fi“.
- Führen Sie Banking-, Shopping- oder andere vertrauliche Transaktionen nur zuhause oder in einem vertrauenswürdigen Netzwerk durch.

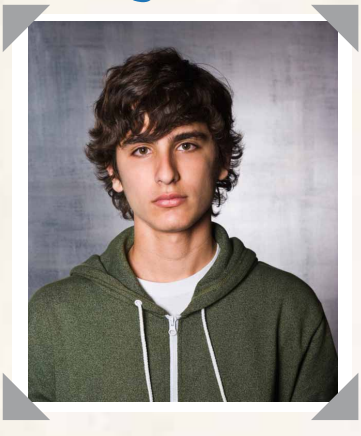
DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Dirk Vielfahrer

VERBRECHEN:
Diebstahl persönlicher Daten

GESUCHT WEGEN:
Wardriving



ALIAS:
Der Kriegsherr, Kalkmeister, Sir Spammeviel

BESONDERE KENNZEICHEN:
Tattoos mit den Symbolen für ein offenes Wi-Fi-Netzwerk

Teilen Sie Ihre Heim-Internetverbindung gern mit völlig Fremden? Sicher nicht. Dirk Vielfahrer tut es.

Er fährt durch Ihre Nachbarschaft und sucht nach Häusern mit offenen oder ungesicherten Drahtlosverbindungen (WLAN-Netzwerken). Er setzt sich einfach an den Straßenrand oder geht an Ihrem Haus vorbei und geht mit seinem Laptop, Smartphone oder Nintendo DS online.

Über Ihre WLAN-Verbindung sendet er dann Spam, sucht im Internet Webseiten mit nicht jugendfreien oder verbotenen Inhalten auf oder schnüffelt in Ihrem Computer herum – auf der Suche nach privaten Informationen, die Sie nicht preisgeben möchten.

Da er dabei Ihre Netzwerkadresse verwendet, kann er seine Aktionen hinter Ihrer Identität verbergen. Und wenn die Polizei ermittelt, klingelt sie an Ihrer Tür.

Erfahren Sie, wie Sie Ihre WLAN-Verbindung schützen können. Für Ihren Schutz können Sie Folgendes tun:

- Ändern Sie den Standardbenutzernamen und das Kennwort, mit denen Ihr Router ausgeliefert wurde. Hacker kennen diese Standarddaten und greifen damit auf ungeschützte Netzwerke zu.
- Deaktivieren Sie die Übertragung Ihrer Router-ID. Damit ist Ihr WLAN für andere unsichtbar.
- Richten Sie Verschlüsselung (mindestens WPA) ein, damit nur Benutzer mit dem richtigen Kennwort auf Ihr Netzwerk zugreifen können.
- Verwenden Sie eine Firewall, damit Datenverkehr von nicht genehmigten Quellen blockiert wird.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Antonio „Big Phish“ Brigante

VERBRECHEN:
Kredit-/EC-Kartenbetrug

GESUCHT WEGEN:
Phishing

ALIAS:
Geldsack, Boss, Spoof, Phish-Köder

BESONDERE KENNZEICHEN:
„Phish“-Haken auf dem linken Oberarm

Dieser „Big Phish“ hat von Ahnungslosen aus aller Welt mehr als 175 Mio. € gestohlen.

Zuerst meldet er sich in Ihrem Posteingang und gibt sich dort als vollkommen legitimer Service-Mitarbeiter einer Bank oder eines Kreditkartenunternehmens aus. Er behauptet dreist, Sie müssten Ihre Datensätze „aktualisieren“ und dazu Ihr Kennwort oder Ihre Kontonummer angeben. Dazu sollen Sie den Webseitenlink öffnen, der in der E-Mail angegeben ist. Antonio ist ein richtiger Profi, deshalb sieht die Webseite wirklich wie die Ihrer Bank aus. Aber die Webseite ist eine raffinierte Fälschung.

Klimper, klimper... Kurz darauf stellen Sie fest, dass Sie neue Kleider für Frau Phish, ein Vier-Sterne-Essen, Luxusurlaub oder eine Yacht für Herrn Phish bezahlt haben, damit er sich einen besonderen Angelurlaub gönnen kann.

Phisher gehen sehr gewieft vor und tarnen sich gut. Für Ihren Schutz können Sie Folgendes tun:

- Ignorieren Sie Nachrichten wie die oben beschriebene, oder informieren Sie Ihre Bank darüber.
- Klicken Sie auf keine unbekannten Links in E-Mails, Sofortnachrichten oder Facebook-Einträgen, weil sie möglicherweise zu gefälschten Webseiten führen.
- Öffnen Sie ein neues Browserfenster (nicht nur eine neue Registerkarte), und geben Sie die URL ein, um die legitime Webseite aufzurufen.
- Verwenden Sie die Software McAfee SiteAdvisor®: Sie bietet Risikobewertungen für Ihre Suchergebnisse.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Willi „Wanderauge“

VERBRECHEN:
Krimineller Datendiebstahl

GESUCHT WEGEN:
Shoulder Surfing

ALIAS:
Schnüffler, Adlerauge, iHabicht, Spanner-Willi

Mit seinen Adleraugen, Ferngläsern oder einer versteckten Kamera schaut dieser Kriminelle den Leuten über die Schulter, während sie am Bankautomaten ihre PIN eingeben, Formulare ausfüllen oder sich in Internet-Cafés bei ihren Konten anmelden.

Willi geht dabei so geschickt vor, dass Sie ihn noch nicht einmal bemerken.

Sobald er Ihre Zahlen ausgespäht hat, speichert er diese vertraulichen Daten und bieten sie in kriminellen Netzwerken in den dunklen Gassen des Internets zum Verkauf an. Diesen Typen wollen Sie wirklich nicht in Ihrer Nähe haben.

Achten Sie auf umherwandernde Augen. Für Ihren Schutz können Sie Folgendes tun:

- Decken Sie immer Ihre Hand bzw. die Eingabemaske ab, wenn Sie Ihre PIN eingeben.
- Wenn Sie im Internet-Café oder öffentlichen Hotspot online gehen, wählen Sie einen Platz direkt mit dem Rücken zur Wand.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Richard „Keylogger“ Kleidermann

VERBRECHEN:
Identitätsdiebstahl

GESUCHT WEGEN:
Keylogger

ALIAS:
Der Pianist, Zarte Hand

Wenn dieser Virtuose in die Tasten haut, sollten Sie vorsichtig sein: Er kann Ihren Computer infizieren und Ihre Online-Aktivitäten überwachen.

Mit künstlerischem Können platziert er seine Software auf unschuldigen Webseiten und wartet auf ahnungslose Web-Touristen. Wenn Sie die Webseiten besuchen, installiert sich seine Software heimlich auf Ihrem Computer und beobachtet anschließend jeden Ihrer Schritte.

Sie speichert – unbemerkt – alle Ihre Tastatureingaben und sendet Herrn Keylogger Kleidermann süße Töne: Benutzernamen, Kennwörter, Bankkonto- sowie Kreditkartennummern. Er weiß, welche Suchbegriffe Sie verwendet und welche Webseiten Sie aufgerufen haben, und erstellt Screenshots, wenn Sie mit Ihrer Maus Sicherheits-Codes markieren.

Unsichtbarkeit ist der Schlüssel für seinen Erfolg. Sie sehen seine Software nicht und installieren den Code auch nicht bewusst. Es gibt keine Hinweise darauf, dass er sich auf Ihrem Computer herumtreibt.

Es gibt Tools, die unerwünschte Software von Ihrem Computer fernhalten. Für Ihren Schutz können Sie Folgendes tun:

- Halten Sie Ihren Web-Browser aktuell, indem Sie die neuesten Patches installieren.
- Verwenden Sie eine umfassende Sicherheits-Software, die sich automatisch aktualisiert und Sie mit einer aktivierten Firewall schützt.

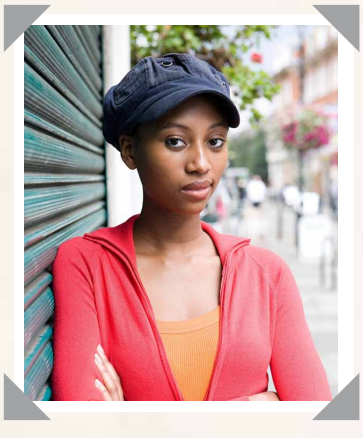
DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

TÄTER:
Polly „Die Plünderin“

VERBRECHEN:
Postbetrug

GESUCHT WEGEN:
Plündern von Briefkästen



ALIAS:
Wühlerin, Briefmarken-Dieb, Die Postlerin

BESONDERE KENNZEICHEN:
Hundebiss von einem Angriff

Die Plünderin ist ganz verrückt nach ungeschützten oder beschädigten Briefkästen und den Briefumschlägen voller persönlicher Informationen, die sie darin findet. Wenn sie den Antrag für eine neue Kreditkarte oder Kreditkartenabrechnungen, Nebenkosten- und Telefonrechnungen, Briefe von der Bank oder Steuerformulare findet, macht sie vor Freude einen Luftsprung.

Mithilfe Ihrer Daten eröffnet sie gefälschte Bank-, Kreditkarten- und Mobiltelefonkonten. Wenn die Bank die Benutzer-ID und das Kennwort für das neue Konto verschickt, kommt Polly wieder. Bei ihren Diebestouren scheut sie selbst vor ihren Nachbarn nicht zurück.

Sie leidet unter einer gespaltenen Persönlichkeit: Sie hat mehr als 10.000 Kreditkartenkonten unter verschiedenen Namen eröffnet und diese Konten mit 350.000 € belastet, ohne dafür einen einzigen Cent zu bezahlen. Viele Opfer haben mehr als ein Jahr nichts geahnt... Genug Zeit, um in Ihrem Namen hohe Schulden anzuhäufen.

Prävention bietet den besten Schutz vor Postdieben. Für Ihren Schutz können Sie Folgendes tun:

- Überwachen Sie Ihren Schufa-Eintrag auf ungewöhnliche Aktivitäten, einschließlich Überprüfungen Ihrer Kreditwürdigkeit und neuen Kreditkarten.
- Lassen Sie sich Kontoauszüge online zustellen, damit sie nicht per Post gesendet werden.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitäts-diebstahl

Adware
Software, die automatisch Werbung auf einem Computer wiedergibt, anzeigt oder herunterlädt. Dabei wird das Surfverhalten überwacht und dazu passende Werbung angezeigt. Adware stellt meist kein Sicherheitsrisiko dar. Es gibt jedoch auch Formen, die als Spyware agieren und Informationen von Ihrer Festplatte, aus den von Ihnen besuchten Webseiten oder sogar aus Ihren Tastatureingaben sammeln. Einige Adware-Formen sind in der Lage, persönliche Daten zu erfassen oder zu übertragen.

Backdoor
Eine Programmfunktion, über die Angreifer unerkannt auf einen anderen Computer zugreifen und ihn fernsteuern können. Programmierer bauen solche Hintertüren oft in Software-Anwendungen ein, damit sie Fehler beheben können. Wenn Hacker oder andere von einer Backdoor erfahren, kann diese Funktion ein Sicherheits-risiko darstellen.

Botnet oder Bot (siehe auch Zombie)
Bezeichnet eine Sammlung von Zombie-Computern, die autonom und automatisch arbeiten. „Botnet" ist eine Kurzform von „Roboter-Netzwerk". Der Computer kann durch einen Hacker, einen Computervirus oder einen Trojaner kompromittiert worden sein. Ein Botnet kann aus

Fortsetzung

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

Zehn- oder sogar Hunderttausenden Zombie-Computern bestehen. Ein einzelner Computer in einem Botnet kann automatisch Tausende Spam-Nachrichten pro Tag senden. Die meisten Spam-Nachrichten stammen von Zombie-Computern.

Browser-Hijacker
Bezeichnet das Ändern von Web-Browser-Einstellungen durch Malware. Der Begriff „Hijacking" (Entführung) wird verwendet, weil die Änderungen ohne Zustimmung des Benutzers durchgeführt werden. Manchmal kann Browser-Hijacking leicht rückgängig gemacht werden, in anderen Fällen jedoch nicht. Häufig werden die Startseite, Suchseite, Suchergebnisse, Fehlermeldungsseiten oder sonstige Browser-Inhalte durch unerwartete oder unerwünschte Inhalte ersetzt, oder es werden Webseiten geöffnet, die der Benutzer gar nicht besuchen wollte.

Carding
Methode zur Überprüfung der Gültigkeit gestohlener Kartendaten. Der Dieb verwendet die Kartendaten auf einer Webseite, über die Transaktionen in Echtzeit verarbeitet werden. Wenn die Transaktion erfolgreich verarbeitet wird, weiß der Dieb, dass die Karte noch gültig ist. Im Allgemeinen wird dabei etwas für einen kleinen Betrag gekauft, um das Limit der Karte nicht auszuschöpfen und nicht den Verdacht des Karteninhabers zu erwecken.

Cybersquatting (Domänenbesetzung)
Bezeichnet das Registrieren, Kaufen und Verkaufen oder Verwenden eines Domänennamens in böswilliger Absicht, um von der Bekanntheit einer Handelsmarke oder eines Markennamens zu profitieren, die/der anderen gehört. Der Cybersquatter bietet die Domäne dann der Person oder dem Unternehmen überteuert zum Kauf an, der bzw. dem die im Domänennamen enthaltene Marke gehört. Manchmal registrieren Cybersquatter auch Varianten bekannter Markennamen. Dies wird als Typosquatting (Tippfehlerdomänen) bezeichnet und dient der Malware-Verbreitung.

Drive-by-Download
Ein Programm, das automatisch ohne Ihre Zustimmung oder sogar ohne Ihr Wissen auf Ihren Computer heruntergeladen wird. Dabei können beim bloßen Öffnen einer E-Mail oder Webseite Malware oder potenziell unerwünschte Programme installiert werden.

Exploit
Eine Software, die einen Fehler oder eine Panne ausnutzt, um unbeabsichtigtes oder unvorhergesehenes Verhalten von Computer-Software zu verursachen. Mithilfe solcher Software können

Fortsetzung

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

Täter zum Beispiel die Kontrolle über ein Computersystem erlangen, Zugriffsrechte verändern oder Benutzern Zugriff oder Ressourcen verweigern.

Firewall
Eine Hard- oder Software, die unbefugte Zugriffe blockiert und lediglich autorisierte Kommunikation zulässt. Sie wird mithilfe einer Reihe von Regeln konfiguriert, in denen festgelegt wird, welche Netzwerkübertragungen zugelassen werden sollen und welche nicht. Firewalls dienen dazu, die Ressourcen des Netzwerks vor Benutzern in anderen Netzwerken zu schützen.

Identitätsdiebstahl bei Kindern
Identitätsdiebe stehlen immer häufiger die Identität von Kindern und sogar Säuglingen, da die Datensätze von Kindern meist keinerlei offizielle Einträge enthalten. Es kann Jahre dauern, bis der Diebstahl entdeckt wird. In vielen Fällen stellen die Opfer den Identitätsdiebstahl erst fest, wenn sie ihre erste finanzielle Transaktion durchführen möchten. Zu den möglichen Gefahren des Identitätsdiebstahls bei Kindern zählen unter anderem geschädigte Kreditwürdigkeit und Haftbarkeit wegen anfallender Einkommenssteuern.

Informationssammler
Personen, die Daten stehlen, sie aber nicht unbedingt selbst für betrügerische Aktivitäten verwenden. Die gesammelten Informationen werden an kriminelle Netzwerke verkauft, die in den dunklen Gassen des Internets damit handeln.

Internetkriminelle
Internetkriminelle sind Hacker, Cracker und andere böswillige Benutzer, die das Internet und Computer mit krimineller Absicht verwenden. Zu den begangenen Verbrechen gehören unter anderem Identitätsdiebstahl, PC-Hijacking, illegales Spamming, Phishing und Pharming.

Kennwort-Sniffing
Bezeichnet die Verwendung eines Tools zur Erfassung von Kennwörtern, die über ein Netzwerk oder über das Internet übermittelt werden. Bei einem Sniffer kann es sich um Hard- oder Software handeln.

Kennwortangriffe
Ein Versuch, die Kennwörter eines Benutzers in Erfahrung zu bringen, um sie anschließend illegal einzusetzen. Vor Kennwortangriffen gibt es nur begrenzten Schutz. Hierzu gehört die Einhaltung folgender Grundregeln: Verwenden Sie Kennwörter mit einer gewissen Mindestlänge sowie ohne sinntragende Wörter, und ändern Sie sie häufig.

Keylogger (oder Keystroke Logger)
Die Überwachung (oder Protokollierung) von Tastaturtasten-

Fortsetzung

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

anschlägen. Dies geschieht meist im Verborgenen, sodass die Person, die die Tastatur verwendet, von der Überwachung ihrer Aktionen nichts erfährt. Dazu werden böswillige Programme eingesetzt, die die Tastenanschläge aufzeichnen. Erfasst werden beispielsweise Sofortnachrichten, E-Mail-Texte, E-Mail-Adressen, Kennwörter, Kreditkarten- und Kontonummern, Adressen sowie andere private Daten.

Krimineller Identitätsdiebstahl
Dieser Sachverhalt liegt vor, wenn ein Täter sich bei einer Verhaftung gegenüber der Polizei mit betrügerischen Methoden als eine andere Person ausweist. In einigen Fällen haben sich Täter zuvor offizielle Identitätsdokumente mit gestohlenen persönlichen Daten verschafft, oder sie legen einfach gefälschte Ausweise vor.

Malware
Malware ist ein allgemeiner Begriff für Software, mit der heimlich auf ein Computersystem zugegriffen werden soll, ohne dass sein Besitzer davon weiß. Zu Malware gehören Viren, Würmer, Trojaner, Spyware und bösartige aktive Inhalte.

Manipulation von Geldautomaten (Skimming)
Bei dieser Betrugsform werden Kontodaten/PINs gesammelt, indem an Geldautomaten Geräte befestigt werden, die die Kartendaten der arglosen Opfer auslesen.

Nicht autorisiertes Programm
Bezeichnet Programme, die andere Programme oder Daten beschädigen oder die Sicherheit eines Computers oder Netzwerks kompromittieren.

Payload (schädlicher Code)
Bezeichnet die schädlichen Auswirkungen von bösartigem Code, der über einen Virus oder eine sonstige Malware ausgeführt wird. Zu Payload-Aktivitäten gehören das Verschieben, Verändern, Überschreiben oder Löschen von Dateien, aber auch andere destruktive Aktivitäten.

Pharming
Bezeichnet das Umleiten von Datenverkehr an eine gefälschte Webseite, häufig mithilfe von Malware oder Spyware. Ein Hacker richtet eine betrügerische, aber legitim aussehende Webseite ein, um von Benutzern vertrauliche Informationen zu sammeln.

Phishing
Hierbei handelt es sich um eine Form krimineller Aktivitäten, bei der E-Mails oder Sofortnachrichten für Social-Engineering-Techniken verwendet werden. Phisher versuchen, auf betrügerische Weise an persönliche Daten anderer Personen zu kommen (z. B. Kennwörter und Kreditkarten-

Fortsetzung

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

daten), indem sie sich in scheinbar offiziellen elektronischen Nachrichten als vertrauenswürdige Personen oder Unternehmen ausgeben. Meist werden die Empfänger von Phishing-E-Mails aufgefordert, auf den Link in der E-Mail zu klicken, um Kontakt- oder Bankdaten zu bestätigen oder zu aktualisieren. Ebenso wie Spam werden Phishing-E-Mails an eine Vielzahl von E-Mail-Adressen gesendet, in der Hoffnung, dass einige Empfänger darauf hereinfallen und ihre persönlichen Informationen preisgeben. Phishing ist auch über Sofortnachrichten oder Telefon möglich (siehe SMiShing oder Vishing).

Piggybacking
Methode zur Erlangung nicht autorisierten Zugriffs auf ein System, indem die legitime Verbindung des Benutzers ohne dessen Zustimmung oder Wissen missbraucht wird.

Postbetrug
Umfasst jedes Vorhaben, bei dem versucht wird, über das Postsystem unrechtmäßig an Geld oder Wertsachen zu kommen. Hierzu gehört der Identitätsdiebstahl durch betrügerischen Adresswechsel oder durch Stehlen von Post (Plündern von Briefkästen).

P2P-Netzwerk (Peer-to-Peer)
Ein verteiltes Dateifreigabesystem, bei dem jeder Computer im Netzwerk für jeden anderen Computer im Netzwerk sichtbar ist. Benutzer können gegenseitig auf die Festplatten zugreifen, um Dateien herunterzuladen. Diese Art der gemeinsamen Nutzung von Dateien kann sinnvoll sein, führt jedoch häufig zu Urheberrechtsverletzungen bei Musik-, Film- und anderen freigegebenen Mediendateien. Die Benutzer sind außerdem für Viren, Trojaner und Spyware anfällig, die in Dateien verborgen sind.

Ransomware
Bösartige Software, die die Festplatte des von ihr infizierten Computers verschlüsselt. Der Hacker erpresst anschließend Lösegeld vom Computerbenutzer im Austausch für die Entschlüsselungssoftware, die die Computerdaten wieder nutzbar macht.

Rootkit
Software, die den Zugriff auf einen Computer ermöglicht und sich dabei vor dem Computerbenutzer versteckt. Hierbei handelt es sich meist um Malware, die ohne Wissen des Benutzers Computerressourcen missbraucht oder Kennwörter stiehlt.

Shoulder Surfing (Schulterblick)
Methode, bei der Kriminelle Informationen erlangen, indem sie das Opfer direkt observieren. Kriminelle können sich Ihre PIN-

Fortsetzung

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

Nummer oder Ihr Kennwort verschaffen, indem sie einfach über Ihre Schulter schauen, während Sie einen Geldautomaten oder Computer benutzen.

SMiShing
Bezeichnet den Einsatz von Social-Engineering-Techniken bei Textnachrichten (vgl. Phishing). Der Name ist von „SMS Phishing" abgeleitet (SMS steht für Short Message Service und bezeichnet die Technologie für Mobiltelefon-Textnachrichten). Beim SMiShing wird mithilfe von Mobiltelefon-Textnachrichten versucht, Sie zum Preisgeben persönlicher Informationen zu verleiten. Die Textmeldung verweist möglicherweise auf eine Webseite oder eine Telefonnummer, die mit einem automatischen Sprachausgabesystem verbunden ist.

Social Engineering
Methode zur Manipulation von Personen, damit diese Aktionen ausführen oder vertrauliche Informationen preisgeben. Diese Betrugsform baut auf direkten Kontakt mit dem Opfer, d. h. der Kriminelle versucht, durch Tricks oder Täuschung das Vertrauen des Opfers zu erlangen, um auf diese Weise Informationen zu erhalten, betrügerische Aktionen durchzuführen oder auf das Computersystem des Opfers zuzugreifen.

Spam
Unerbetene oder unerwünschte elektronische Massennachrichten. Spam erreicht seine Opfer per E-Mail, Instant Messaging, Suchmaschinen, Blogs, soziale Netzwerke und Textnachrichten. Spam umfasst seriöse Werbung, irreführende Werbung sowie Phishing-Nachrichten, die Empfänger so hinters Licht führen, dass diese persönliche und finanzielle Daten preisgeben. E-Mails, für deren Empfang sich ein Benutzer extra registriert hat, gelten nicht als Spam.

Spim
Instant-Messaging-Spam. Bei diesen Nachrichten kann es sich einfach um unerbetene Werbung, aber auch um betrügerische Phishing-Nachrichten handeln.

Spyware
Software, die von Hackern heimlich auf Ihrem Computer installiert wird und dazu dient, ohne Ihr Wissen persönliche Informationen zu sammeln. Neben der Überwachung Ihrer Computeraktivitäten kann sie auch dazu eingesetzt werden, Sie auf gefälschte Webseiten zu leiten, Ihre Einstellungen zu ändern oder in anderer Weise die Kontrolle über Ihren Computer zu erlangen.

Fortsetzung

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE

Glossar zum Thema Identitätsdiebstahl

Trojaner
Scheinbar legitimes, aber in Wirklichkeit böswilliges Programm, das unberechtigten Zugriff auf das Computersystem des Opfers ermöglicht. Benutzer werden meist über Tricks dazu verleitet, diese Programme auf ihre Systeme herunterzuladen und anschließend auszuführen. In der Regel wird ein Trojaner aktiv per E-Mail verschickt, d. h. er verschickt sich nicht selbst. Trojaner können auch in Downloads von Webseiten oder P2P-Netzwerken enthalten sein.

Typosquatting (auch URL-Hijacking)
Hierbei handelt es sich um eine Form des Cybersquatting, die sich darauf verlässt, dass Internetnutzer beim Eingeben von Webseitenadressen in die Browser-Adresszeile Schreibfehler machen. Wenn der Benutzer versehentlich eine falsche Webseitenadresse eingibt, wird möglicherweise eine alternative Webseite geöffnet, die einem Cybersquatter gehört.

Vishing (siehe auch Phishing)
Eine kriminelle Aktivität, bei der eine scheinbar legitime Quelle über ein Telefonsystem versucht, an Informationen zu gelangen (Phishing per Telefon/Voicemail). Diese Anrufe werden über VoIP (Voice Over IP) getätigt, da auf diese Weise Anrufer-IDs gefälscht werden können und der Zugang zu persönlichen und finanziellen Informationen vereinfacht wird.

Wardriving
Diebstahl persönlicher Informationen durch Herumfahren auf der Suche nach ungesicherten Drahtlosverbindungen (WLAN-Netzwerken) mithilfe eines tragbaren Computers oder PDAs (Personal Digital Assistant). Wenn Ihr Heimnetz ungesichert ist, können die Diebe auf die Daten aller am WLAN-Router angeschlossenen Computer zugreifen sowie die Daten erfassen, die Sie auf Online-Banking- und Kreditkarten-Webseiten eingeben.

Wühlen im Abfall
Das Durchsehen des Abfalls von Firmen oder Privathaushalten in der Hoffnung, Informationen zu finden, die für Diebstahl oder in betrügerischer Absicht verwendet werden können.

Zombie
Ein Computer, der von einem Virus oder Trojaner kompromittiert wurde und vom Online-Hijacker ferngesteuert wird. Der Hijacker nutzt den Zombie zum Generieren von Spam oder manipuliert den Computer so, dass er für den Besitzer unbrauchbar wird. In den meisten Fällen ist sich der Computernutzer nicht bewusst, dass er kompromittiert wurde. Ein kompromittierter Computer ist meist Teil eines großen Botnets und wird per Fernsteuerung für böswillige Aktionen missbraucht.

DIE MEISTGESUCHTEN IDENTITÄTSDIEBE