
بسم الله الرحمن الرحيم

دانشگاه الزهرا

پژوهشکده زنان

روندهای جرائم سایبری در جهان

ارائه: علی عزیزی دانشیار بازنشسته دانشگاه جامع علوم انتظامی امین

پاییز ۱۴۰۳

شما بانوان نخبه، دختران نخبه، جوانان نخبه، یکی از مهمترین مسئولیت یاتان امروز این است که نقش زن را از دیدگاه اسلام ترسیم کنید، برجسته کنید، روشن کنید.
(مقام معظم رهبری)

مرکز مطالعات راهبردی فرماندهی انتظامی جمهوری اسلامی ایران

دانشگاه الزهرا (س)
پژوهشکده زنان

دانشگاه الزهرا (س)
معاونت فرهنگی و اجتماعی

زنان

فرهنگ؛ انتظام؛ امنیت و تمدن سازی

پژوهشکده زنان با همکاری معاونت فرهنگی و اجتماعی دانشگاه الزهرا (س)
"سومین پیش‌نشست همایش ملی زنان؛ فرهنگ؛ انتظام ؛ امنیت و تمدن‌سازی"
برگزار می‌کند

سخنرانان:

سردار دکتر داود معظمی کودرزی
رئیس پلیس فتا، فرماندهی انتظامی تهران بزرگ
موضوع: تهدیدات فضای مجازی و شبکه‌های اجتماعی

دکتر علی محمد رجبی
رئیس مرکز تشخیص و پیشگیری پلیس فتا
موضوع: اینستاگرام و جرایم دختران

دکتر علی عزیزی
مدرس دانشگاه جامع علوم انتظامی امین
موضوع: روند پیشگیری از جرایم سایبری در ایران و جهان

ساختمان خوارزمی، طبقه همکف،سالن دکتر تورانی
یکشنبه ۱۴۰۳/۰۹/۱۸ ساعت ۱۳ الی ۱۵
لینک آپارات: https://www.aparat.com/alzahrauniversity/live

همایش ملی زنان :

فرهنگ، انتظام، امنیت و تمدن سازی

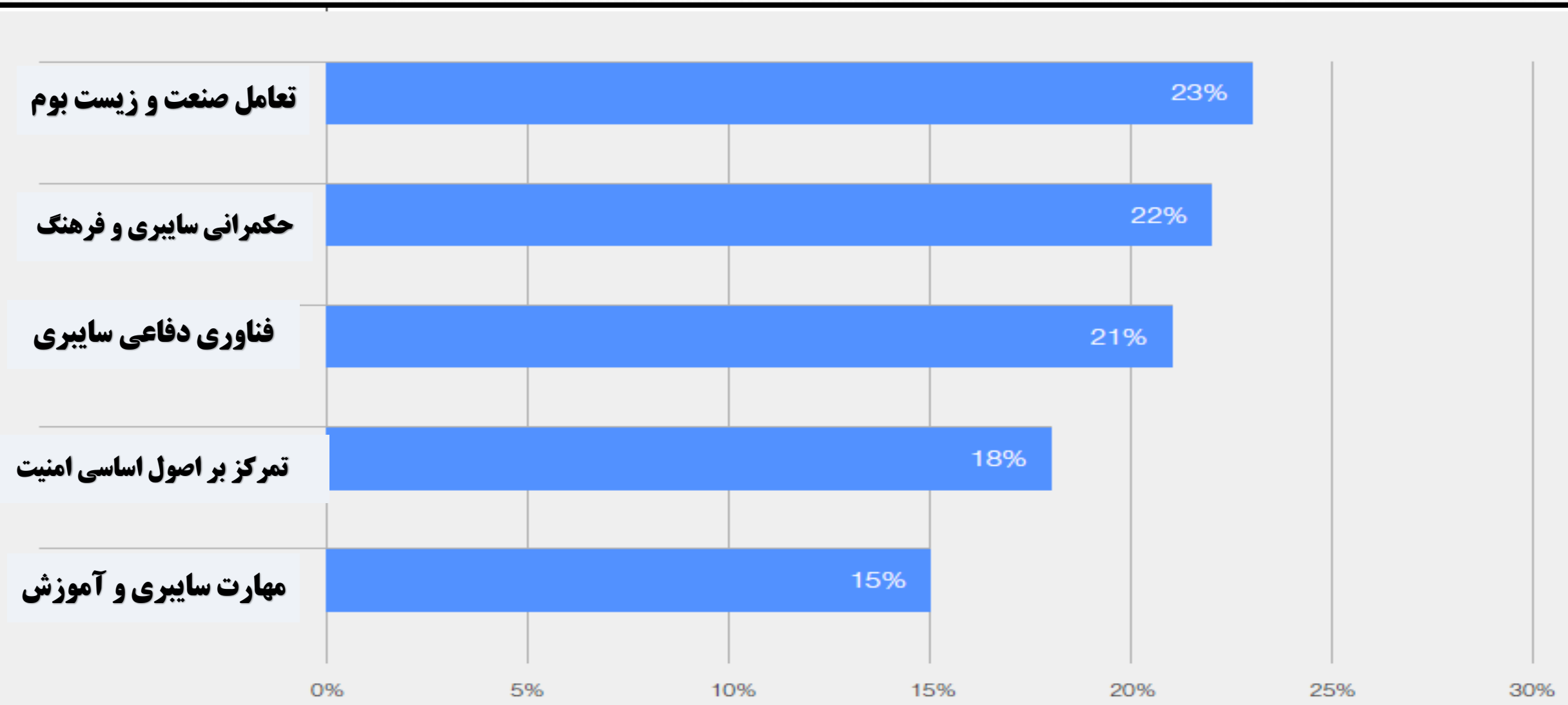
مقدمه:

دنیای امروز جامعه‌ای اطلاعات محور و اصلی ترین عنصر آن «اطلاعات و ارتباطات» است. پیشرفت سریع فناوری اطلاعات و انتقال تجربیات بشری از حوزه سخت افزار به تشکیل دنیای جدیدی به نام فضای مجازی یا فضای سایبری منجر شده است. جوامع مختلف با تأثیرپذیری از تحول بسیار عظیم علمی و تکنولوژیک، به سمت، جامعه اطلاعاتی یا جامعه شبکه‌ای در حال حرکت هستند. جامعه شبکه‌ای به جامعه ای گفته می‌شود که که ساختار آن از فناوری تأثیر پذیرفته است. فناوری های نوین ارتباطات و فضای مجازی نقاط مختلف را در شبکه های جهانی به هم پیوند می‌دهند . شبکه های ارتباطی مجموعه ای از جوامع مجازی را به‌وجود می‌آورند و درنتیجه، آن همه ساختارها و فرآیندهای مادی و معنوی بشری دگرگون می‌شوند.

امروزه، فضای مجازی به طور به‌سزایی در ارتباطات جهانی نقش ایفا می‌کند و به صورت روزافزونی با زندگی مردم همبستگی یافته است.

شبکه‌های اجتماعی مجازی به دلیل عواملی چون عمومیت یافتن در میان کاربران و گستره وسیع جغرافیایی در درون مرزهای ملی ، تبدیل شدن به ارتباطی خصوصی و شخصی و فارغ بودن از هر نوع کنترل از طرف مراجع قدرت، به وسیله‌ای بی بدیل در عرصه ارتباطات تبدیل شده اند و زمینه‌های تأثیرگذاری خارج از کنترل دولت ها و نهادهای قدرت را در جوامع به‌وجود آورده‌اند.

وضعیت تاب آوری حکمرانی



عوامل زمینه ای احتمالی مرتبط با افزایش جرایم سایبری

KINDS OF THREATS

انواع تهدید

INTERCEPTION

AN UNAUTHORIZED PARTY (HUMAN OR NOT) GAINS ACCESS TO AN ASSET

INTERRUPTION

AN ASSET BECOMES LOST, UNAVAILABLE, OR UNUSABLE

MODIFICATION

AN UNAUTHORIZED PARTY CHANGES THE STATE OF AN ASSET

FABRICATION

AN UNAUTHORIZED PARTY COUNTERFEITS AN ASSET

رهگیری

دسترسی یک طرف غیرمجاز (انسانی یا غیر انسانی) به یک دارایی

وقفه

مفقود شدن، در دسترس نبودن، یا غیرقابل استفاده بودن یک دارایی

تغییر

تغییر وضعیت یک دارایی از طرف یک طرف غیرمجاز

جعل

جعل یک دارایی از سوی یک طرف غیرمجاز


دفاع سایبری

METHODS OF DEFENSE

روش های دفاع

FIVE BASIC APPROACHES TO DEFENSE OF COMPUTING SYSTEMS

PREVENT ATTACK

BLOCK ATTACK / CLOSE VULNERABILITY

DETER ATTACK

MAKE ATTACK HARDER (CAN'T MAKE IT IMPOSSIBLE ☹)

DEFLECT ATTACK

MAKE ANOTHER TARGET MORE ATTRACTIVE THAN THIS TARGET

DETECT ATTACK

DURING OR AFTER

RECOVER FROM ATTACK

پنج رویکرد اساسی برای دفاع از سیستم های پردازش

پیشگیری از حمله

مسدود کردن حمله / آسیب پذیری

بازدارندگی در برابر حمله

سخت تر کردن حمله (نمی توان آن را غیرممکن کرد)

منحرف کردن حمله

قرار دادن هدف جذاب تری از هدف اصلی

شناسایی حمله

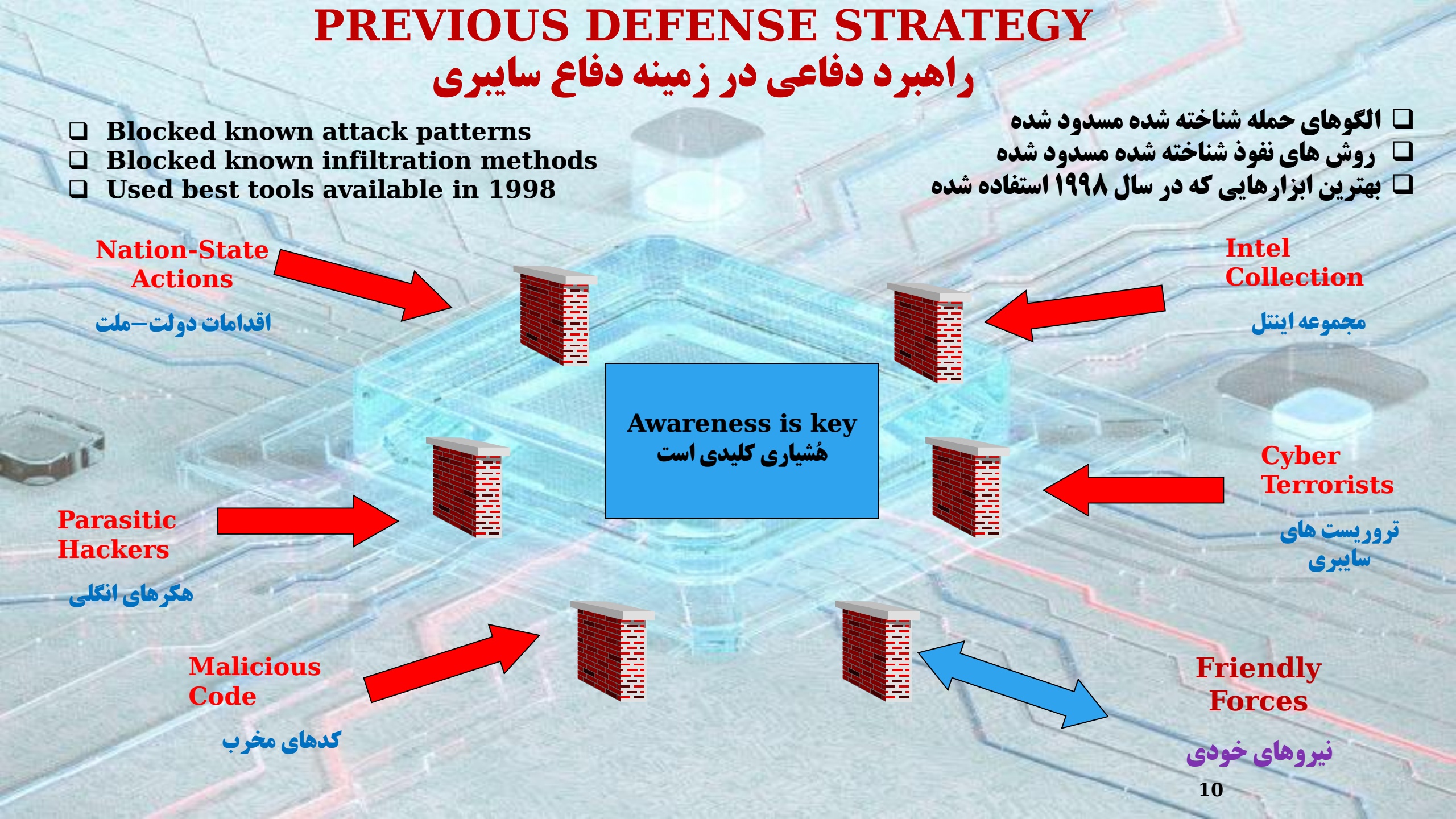
در حین یا بعد از حمله

بازیابی بعد از حمله

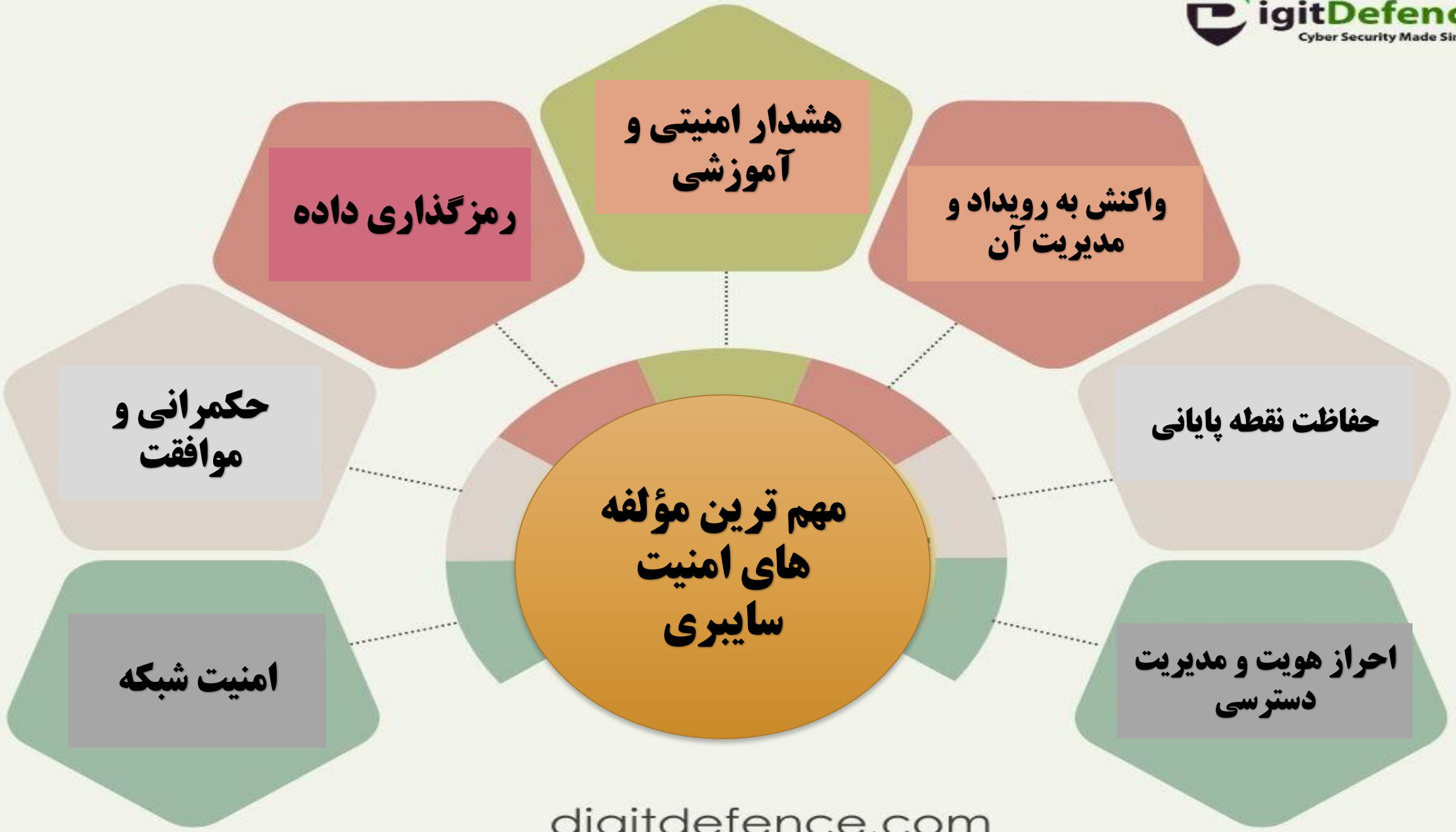
PREVIOUS DEFENSE STRATEGY
راهبرد دفاعی در زمینه دفاع سایبری

- Blocked known attack patterns
- Blocked known infiltration methods
- Used best tools available in 1998

- الگوهای حمله شناخته شده مسدود شده
- روش های نفوذ شناخته شده مسدود شده
- بهترین ابزارهایی که در سال ۱۹۹۸ استفاده شده




امنیت سایبری
Global Cybersecurity Outlook 2023 12


DigitDefence
Cyber Security Made Simple.
مهم ترین مؤلفه های امنیت سایبری
هشدار امنیتی و آموزشی
واکنش به رویداد و مدیریت آن
حفاظت نقطه پایانی
احراز هویت و مدیریت دسترسی
امنیت شبکه
حکمرانی و موافقت
رمزگذاری داده
digitdefence.com

HOW MUCH SECURITY IS ENOUGH?

چه میزان امنیت کافی است؟

WE IMPLEMENT SECURITY BASED ON COST VS. RISK

- **THREAT * VULNERABILITY = RISK**
- **COST OF IMPLEMENTING CONTROLS – COST OF NOT IMPLEMENTING CONTROLS = COST**

پیاده سازی امنیت را بر اساس هزینه در مقابل ریسک

تهدید * آسیب پذیری = ریسک

هزینه اجرای کنترل ها – هزینه عدم اجرای کنترل ها = هزینه

ATTACKERS

مهاجمان

ATTACKERS NEED MOM

METHOD

SKILL, KNOWLEDGE, TOOLS, ETC. WITH WHICH TO PULL OFF AN ATTACK

OPPORTUNITY

TIME AND ACCESS TO ACCOMPLISH AN ATTACK

MOTIVE

REASON TO PERFORM AN ATTACK

مهاجمان به MOM نیاز دارند

روش

مهارت، دانش، ابزار که مهاجم با آن حمله را انجام می دهد

فرصت

زمان و دسترسی برای انجام یک حمله

انگیزه

رغبت برای انجام حمله

BASIC COMPONENTS OF SECURITY: CONFIDENTIALITY, INTEGRITY, AVAILABILITY (CIA)

مولفه های اساسی امنیت:

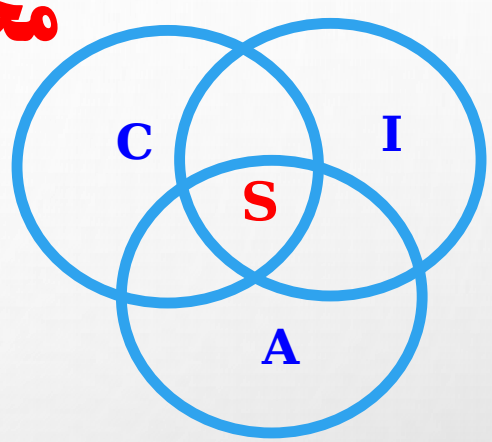
محرمانه‌گی، صحت، در دسترس بودن (سی آی ای)

C-I-A

CONFIDENTIALITY: WHO IS AUTHORIZED TO USE DATA?

INTEGRITY: IS DATA „GOOD?”

AVAILABILITY: CAN ACCESS DATA WHENEVER NEED IT?



S = Secure

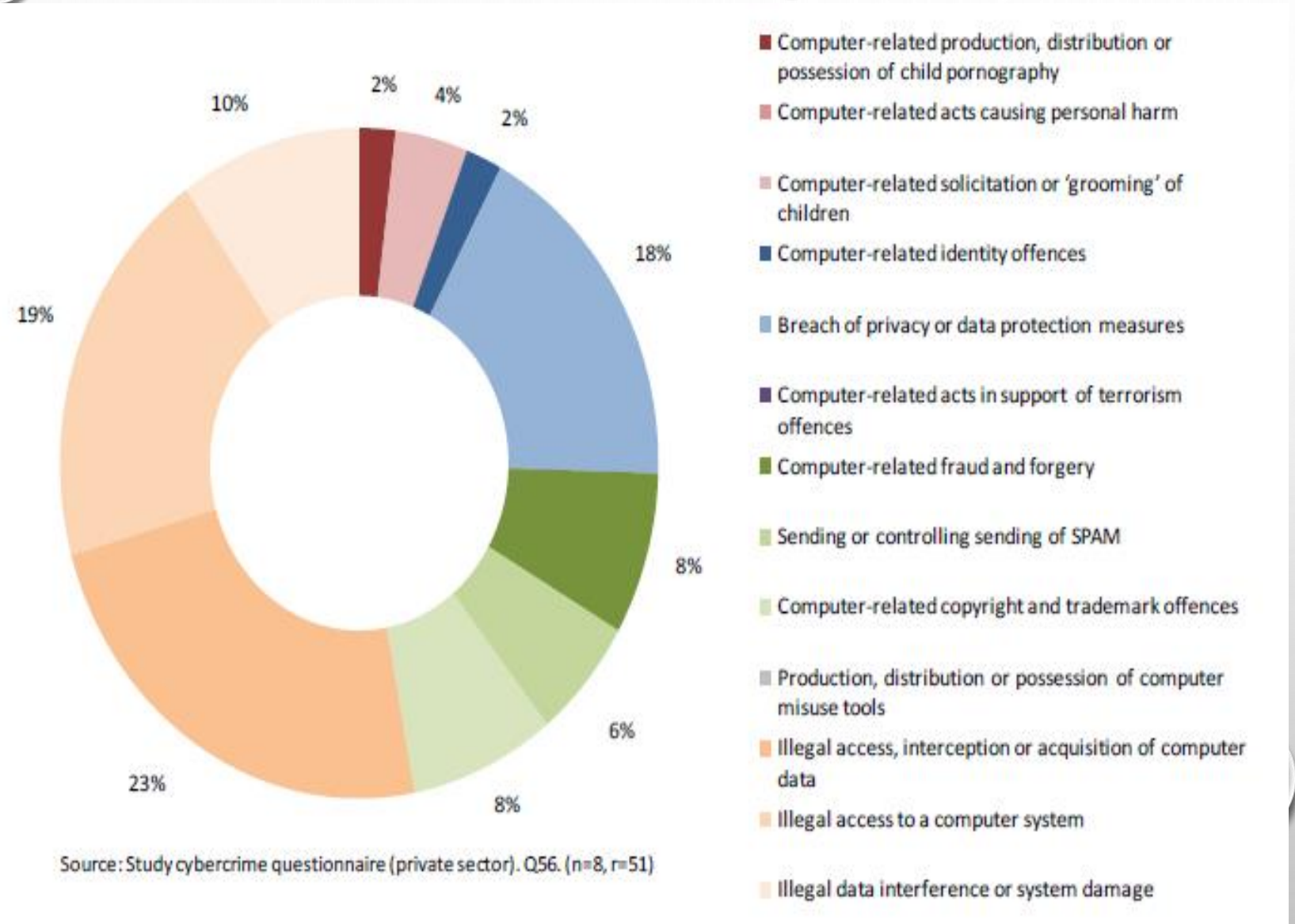
- **CIA or CIAAAN… ☺**

  (other security components added to CIA)

  - **Authentication**
  - **Authorization**
  - **Non-repudiation**
  - **…**

- ❑ احراز هویت
- ❑ مجوز
- ❑ عدم انکار

مهم ترین تهدیدات جرایم سایبری – دیدگاه های سازمان های بخش خصوصی



تولید، توزیع یا در اختیار داشتن پورنوگرافی کودکان مرتبط با رایانه

اعمال مرتبط با رایانه که باعث آسیب شخصی می شود

درخواست یا «تشویق» کودکان به ارتباط با رایانه

جرایم هویتی مرتبط با رایانه

نقض حریم خصوصی یا اقدامات حفاظت از داده ها

اقدامات مرتبط با رایانه در حمایت از جرایم تروریسم

کلاهبرداری و جعل رایانه ای

ارسال یا کنترل هرزنامه

تخلفات مربوط به حق چاپ و علائم تجاری مربوط به رایانه

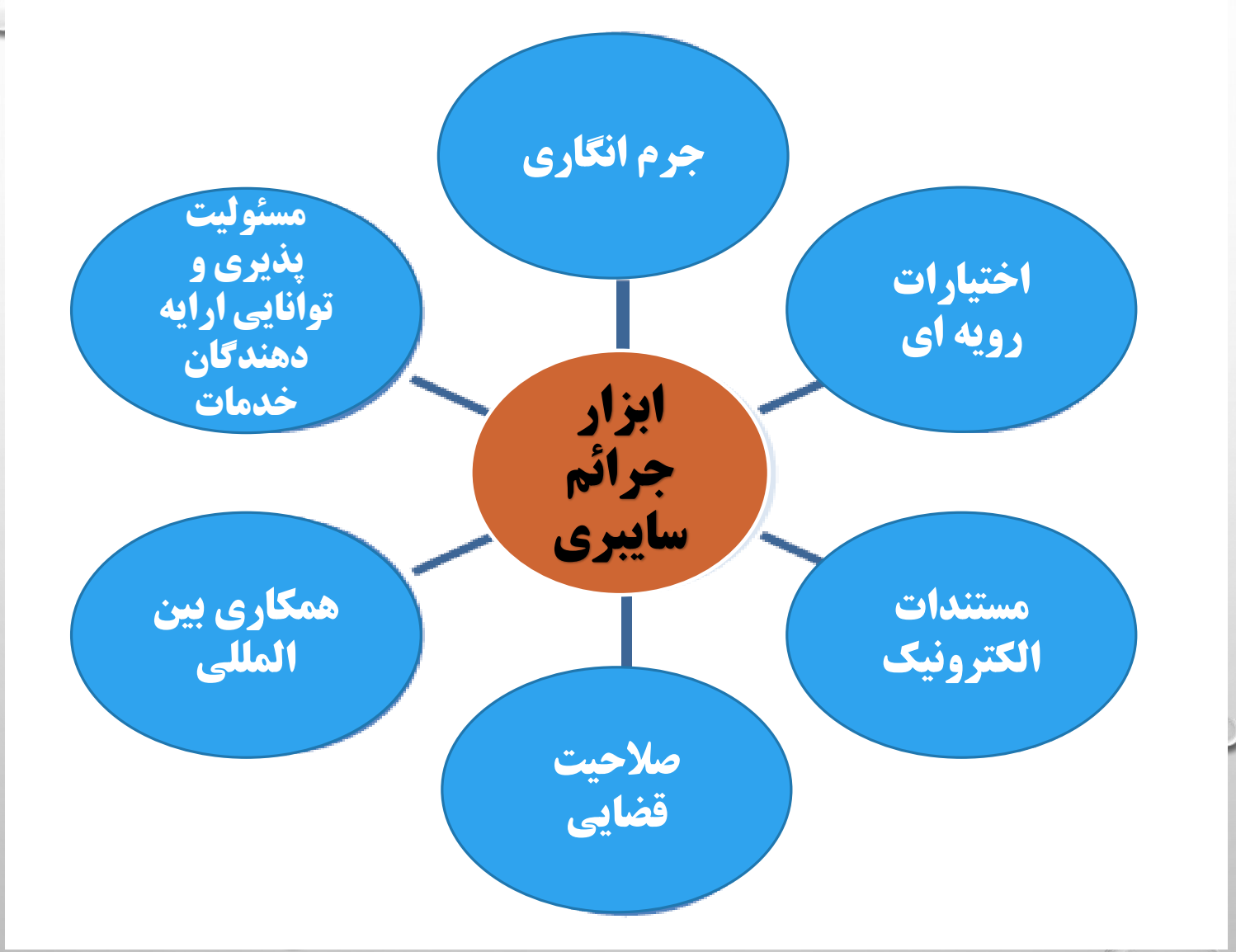
تولید، توزیع یا در اختیار داشتن ابزارهای سوء استفاده از رایانه

دسترسی غیرقانونی، رهگیری یا کسب اطلاعات رایانه ای

دسترسی غیرقانونی به سیستم رایانه ای

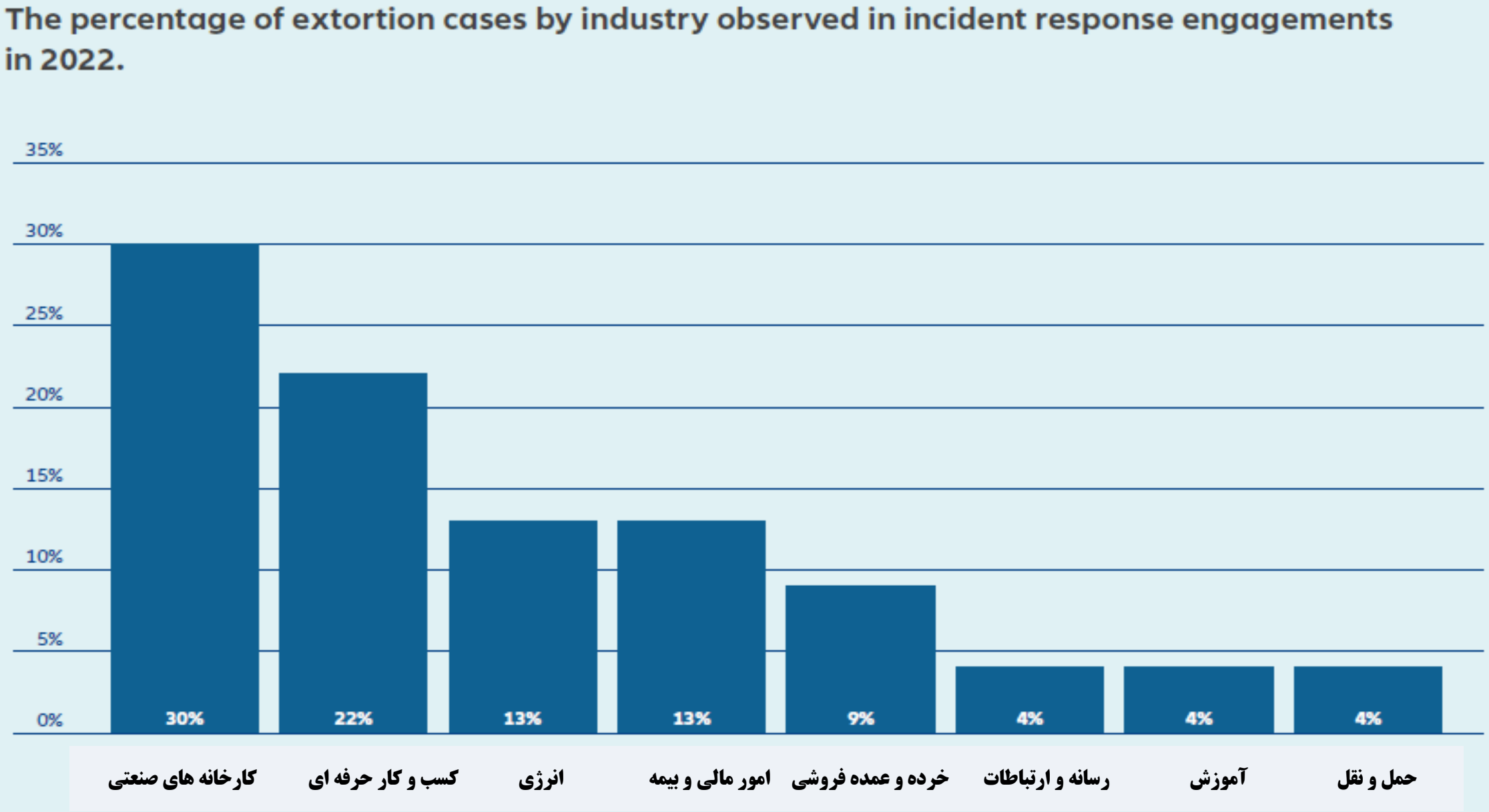
تداخل غیرقانونی داده یا آسیب به سیستم

تمرکز اساسی مستندات قانونی جرایم سایبری



روندهای جرائم سایبری

درصد اخاذی سایبری در سال ۲۰۲۲ از مراکز مهم که منجر به واکنش شده است

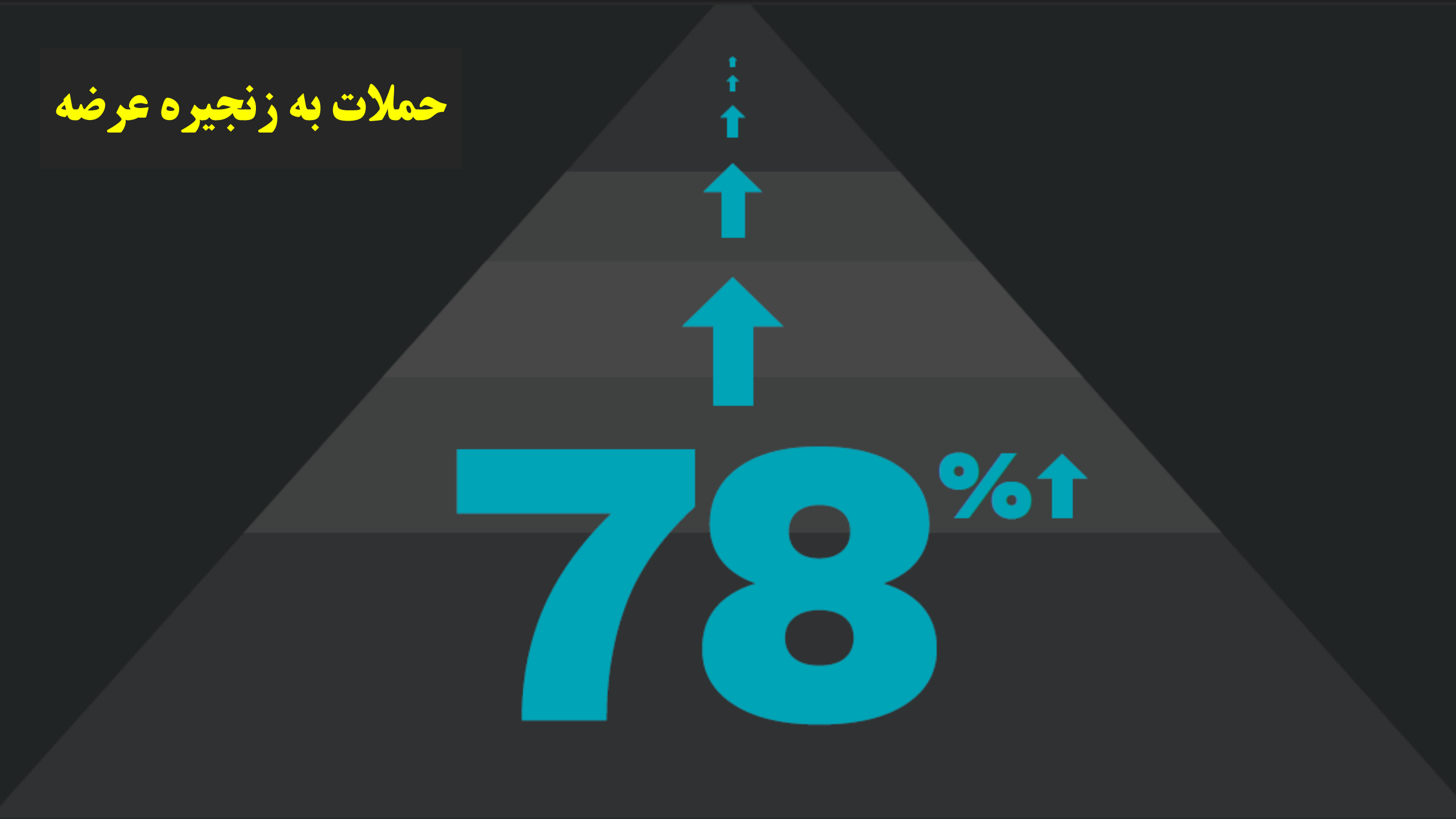


باج افزار در امور سرمایه گذاری

باج افزار از طریق تلفن همراه

مجموع باج افزار

حملات به زنجیره عرضه



ایمیل های مخرب

٪۴۸

از ضمیمه‌های ایمیل مخرب، فایل‌های آفیس هستند که نسبت به ۵ درصد در سال ۲۰۱۷ افزایش یافته است

پاورشل

پاورشل یعنی دور زدن سیستم عامل برای در دست گرفتن سیستم توسط عامل انسانی یا ربات

میانگین تعداد سازمان هایی که توسط هر گروه مهاجم هدف قرار گرفته اند.

55

تعداد گروه‌های مهاجم که از بدافزارهای مخرب استفاده کرده اند.

25%

گوشی همراه

افزایش ۳۳ درصدی گوشی های همراه، با آلودگی باج افزار از سال ۲۰۱۷

بر روی هر

گوشی همراه، روی یک گوشی همراه اپلیکیشن با ریسک بالا نصب شده است.

اهداف مورد حمله

اتهامات جاسوسی توسط مقامات ایالات متحده به:

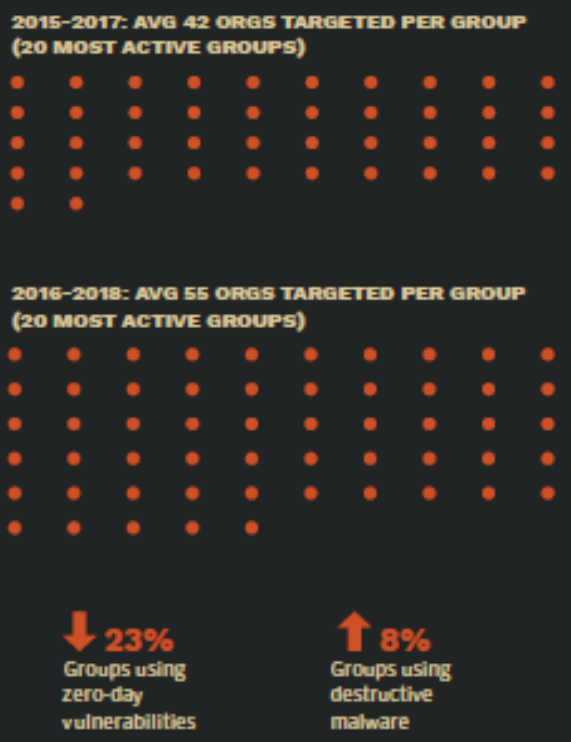
۴۹

- ۱۹ چین
- ۱۸ روسیه
- ۱۱ ایران
- ۱ کره شمالی

۲۰۱۸

۴

۲۰۱۷



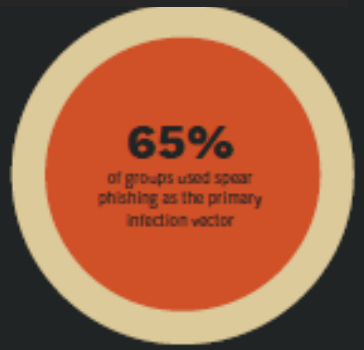
انگیزه اصلی ۹۶ درصد از گروه ها، جمع آوری اطلاعات است

جمع آوری اطلاعات

۵

۲۰۱۶

فیشینگ نیزه



۶۵ درصد از گروه ها از نیزه فیشینگ به عنوان آلودگی اولیه استفاده کردند

ده نوع کلاهبرداری نگران کننده

1
کلاهبرداری شغلی
2022 2,944
2023 5,737

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$79.4 MILLION

2
کلاهبرداری تجارت الکترونیک
2022 1,989
2023 4,516

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$7.3 MILLION

3
کلاهبرداری از طریق مکالمه جعلی
2022 633
2023 3,855

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$12.6 MILLION

4
کلاهبرداری از طریق فیشینگ
2022 2,322
2023 2,991

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$7.4 MILLION

5
کلاهبرداری سرمایه گذاری
2022 1,573
2023 1,598

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$97 MILLION

6
کلاهبرداری جعل هویت از طریق شبکه های اجتماعی
2022 901
2023 524

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$4.6 MILLION

7
کلاهبرداری از طریق عشق اینترنتی
2022 443
2023 446

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$25.9 MILLION

8
کلاهبرداری از طرق وام
2022 545
2023 427

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$2.7 MILLION

9
کلاهبرداری جعل عنوان مقامات دولتی
2022 320
2023 369

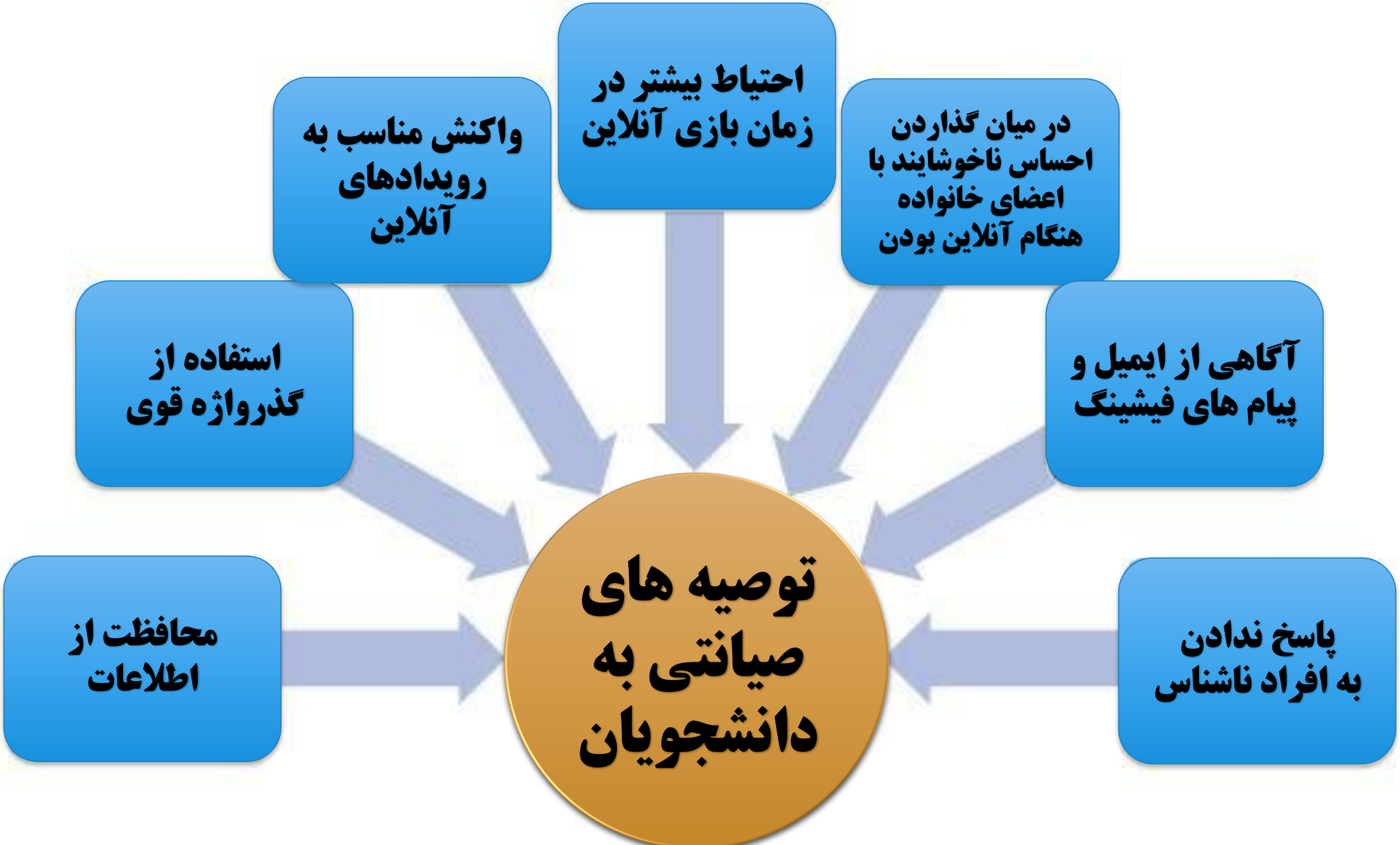
TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$42.8 MILLION

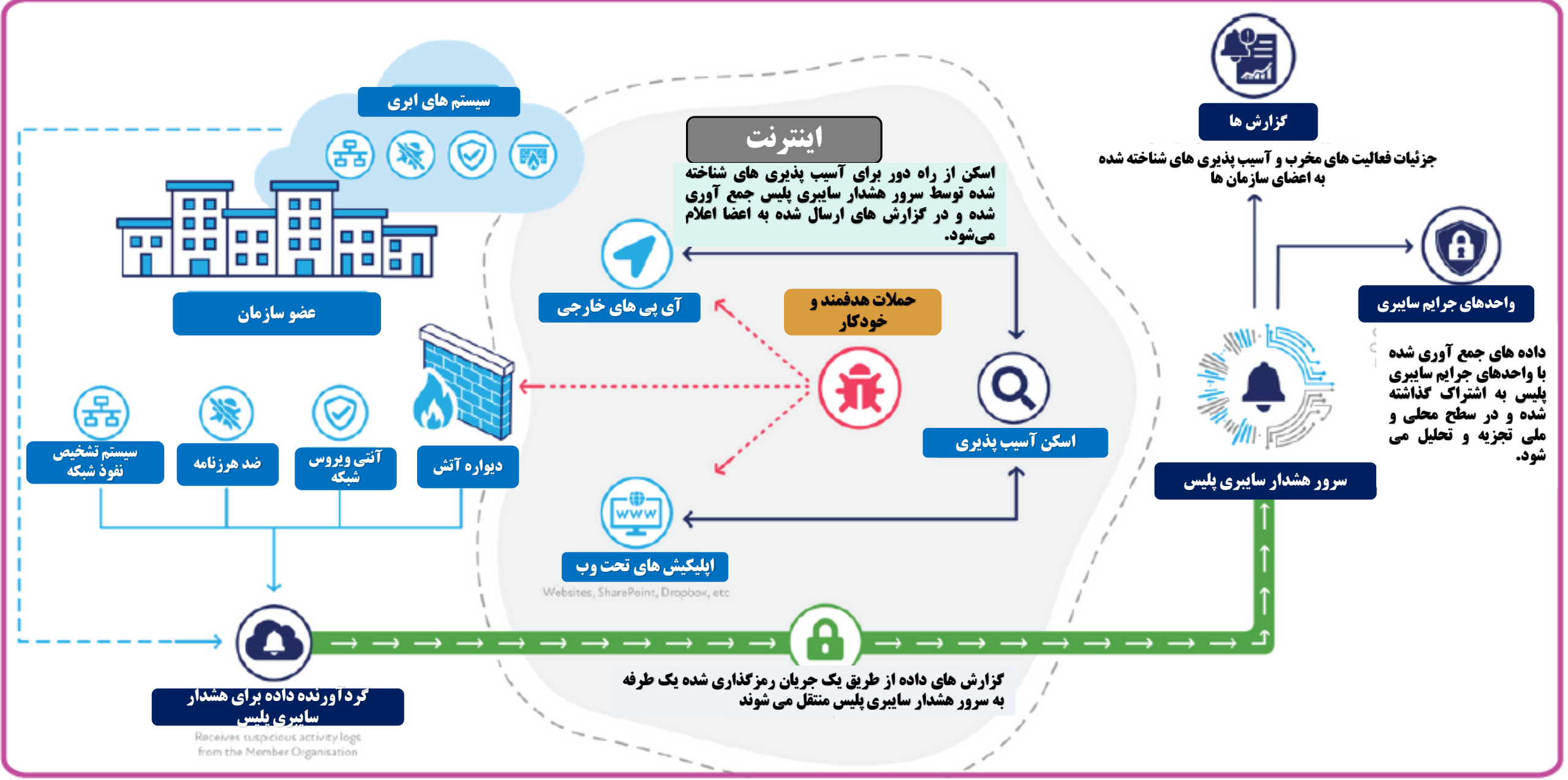
10
اعتبار برای کلاهبرداری جنسی
2022 314
2023 361

TOTAL AMOUNT REPORTED TO HAVE BEEN CHEATED
$1.3 MILLION

Top 10 scams of concern in Singapore according to the Singapore Police Force.


راهکارها


احتیاط بیشتر در زمان بازی آنلاین
واکنش مناسب به رویدادهای آنلاین
در میان گذاردن احساس ناخوشایند با اعضای خانواده هنگام آنلاین بودن
استفاده از گذرواژه قوی
آگاهی از ایمیل و پیام های فیشینگ
توصیه های صیانتی به دانشجویان
محافظت از اطلاعات
پاسخ ندادن به افراد ناشناس



Visual representation of how the UK's Police CyberAlarm works.
Image source: https://cyberalarm.police.uk/police-cyber-alarm/how-it-works/

با تشکر از توجه شما؛

پرسش ؟؟؟