גניבת זהויות באינטרנט וקנייה בטוחה:

גניבת זהויות באינטרנט תופסת תאוצה בשנים האחרונות ומביאה להפסדים גדולים בקרב אנשים וצרכנים שונים הגולשים באינטרנט.
השיטות העיקריות לגניבת זהות הן הוצאת כרטיס אשראי, פתיחת חשבון בנק או לקיחת הלוואה על שמו של אדם אחר. מנתוני חברת המחקר גרטנר עולה, כי בארצות הברית לבדה נפגעו מתרמיות מחשב כ-57 מיליון משתמשים בהיקף של מעל מיליארד דולר בשנת 2005, כ-28% יותר מהשנה הקודמת .[1]

אחת מטכנולוגיות התרמית הנפוצות והבולטות ביותר היא הפישינג (Phishing).
פישינג- היא הונאה שבה נוכלים שולחים הודאות אלקטרוניות מכתובת הדומה לאתר רשמי ומוכר (כמו בנק או חנות מכוונת) ומנסים להוציא פרטים אישיים מהנמענים כגון: כתובת אלקטרונית פעילה, סיסמאות גישה שונות, פרטי כרטיס אשראי וכד'.
לפי ארגון ה- APWG (Anti-Phishing Working Group) אירעו בחודש מאי 2006 מספר שיא של 20,109 התקפות Phishing באמצעות הדואר האלקטרוני, כ-15% יותר מאשר בחודש אפריל .לפי דו"ח השוואתי חצי שנתי של איומי אבטחת מידע שפורסם על ידי חברת סימנטק עולה, כי איומי קוד זדוני העלולים לחשוף מידע חסוי גדלו ב-6% בחצי השנה הקודמת והגיעו ל-80% מכלל איומי האבטחה במחצית השנייה של 2005 CyberSource . העריך, כי ב-2005 הפסידו סוחרים 2.8 מיליארד דולר, עקב הונאות מקוונות.[2]

איך נעשית הונאת פישינג (Phishing)?

נוכלים שולחים כמות גדולה מאוד של דואר אלקטרוני מכתובות של אתרים מוכרים, אבל עם שינוי קל מאוד בשם הדומיין (שם האתר) לדוג': הודעה שנשלחה מ"בנק החבצלת" במקום "בנק חבצלת", או מחנות מקוונת "בונים וקונים" במקום "קונים ובונים".

הודעות ששלחו המתחזים מכילות קישור לאתרים מזוייפים, אל האתרים המזוייפים מגיעים הגולשים בעזרת לחיצה על הקישור שמצורף בהודעה. האתרים דומים מאוד בעיצוב שלהם לאתר המקורי ולפעמים אף זהים לו, פעמים רבות שורת הכתובת שבדפדפן מראה שהגולש נמצא לכאורה באתר המוכר בעוד שלמעשה מדובר בתמונה המסתירה את הכתובת

[1] http://www.gov.il/FirstGov/SafeSurfing/General/SSStealingIdentityNet

[2] http://www.gov.il/FirstGov/SafeSurfing/General/SSStealingIdentityNet

האמיתית. הגולשים מתבקשים להציג באתר המדומה פרטים אישיים שונים כגון: כתובת אלקטרונית פעילה, מספר כרטיס אשראי, מספר תעודת זהות, סיסמאות גישה שונות וכד'.

צורה נוספת להודעת פישינג במייל הינה, קבלת הודעת תשובה (reply) להודעות שלא נשלחו על ידך, ומשלובות עם קובץ או לינק בגוף ההודעה אותו הלינק מעביר אותך אל האתר המזוייף.

קבלת הודעה של עדכון אבטחה או עדכון תוכנה. דבר ראשון עלינו לבדוק האם יש ברשותנו תוכנה מסוג זה, בנוסף למרבית התוכנות שברשותך המחשב מבצע עדכון אוטומטי הנעשה בתוך התוכנה. במידה והינך מעוניין לדעת אם מדובר בעדכון לגיטימי עליך להיכנס בנפרד לאתר של התוכנה ולהוריד את העדכון דרך האתר.

<u>הנזקים השונים העלולים להיווצר כתוצאה ממסירת פרטים אישיים</u>

מהרגע שאתם מוסרים את הפרטים האישיים שלכם לידי הנוכלים, הם יכולים לבצע עם פרטים אלו אין ספור דברים, החל מקניית מוצרים שונים בעזרת כרטיס האשראי שלכם ועד לחובות של אלפי דולרים לגופים שונים. במקרים גרועים יותר אפשר לגלות לפתע שאתם חשודים במתן פרטים שונים לארגוני טרור.

<u>איך מתגוננים מפני פישינג (Phishing)?[3]</u>

- לעולם אל תספקו מידע אישי בתגובה לבקשה שהגיעה בדואר האלקטרוני.
- אם בכל זאת קיבלתם הודעה עם לינק בתוכה, אל תלחצו עליו. היכנסו לאתר באופן עצמאי על ידי הקלדת הכתובת המלאה ותראו לאן הדפדפן לוקח אותכם. גם באתר אליו תגיעו אל תספקו מידע אישי כלשהו.
- אם אתם עדיין לא בטוחים אם מדובר באתר מזוייף או אמיתי תוכלו לשלוח מייל למנהל האתר ולבקש ממנו הבהרות
- התקשרו לגוף ששלח לכם את ההודעה וברורו אם אכן הוא זה ששלח לכם דואר אלקטרוני.
- בדקו כל חודש את החיובים בכרטיס האשראי.
- הקפידו לעדכן את מערכת ההפעלה, הדפדפן ותוכנת האנטי וירוס.

[3] http://www.microsoft.com/israel/athome/security/email/spear_phishing.mspx

דרכים נוספות לגניבת זהויות:

האינטרנט אינו מהווה זירה בלעדית לגניבת זהויות, "גניבת זהות" מאדם מסויים יכולות להתבצע במגוון מקומות שונים.
אנשים רבים אינם מודעים לעובדה כמה קל לבצע היום גניבת זהות גם מבלי לבצע פריצה אל תוך ביתנו. גנב עלול לבחון אותך כאשר אתה מקיש את הקוד הסודי של כרטיס האשראי או להאזין לך מוסר את מספר האשראי בעסקה טלפונית כלשהי. גם האזור סביב ביתנו אינו מוגן. גנבי זהות ועבריינים עלולים לחפש בפחי הזבל של הבניין או במכולות ריקון גדולות בחיפושים אחר פרטים מזהים, פנקסי צ'קים גמורים או צק קרוע שנזרק לפח, טפסים מחברות האשראי אשר נזרקו ללא גריסה ומידע נוסף אשר מכיל פרטים אישיים כמו מספר טלפון כתובת מדויקת, מרשמים וקופסות תרופות מבתי המרקחת וקופות החולים וכד'. מידע כזה עוזר לגנב הזהות להשתלט על חשבונות בשמך ולהשתמש בזהותך.[4]

נפלתם קרבן לגניבת זהות?

אם אתם חוששים כי נפלתם קרבן לגניבת זהות עליכם לפעול מיידית על מנת לצמצם את הנזק הכספי והתדמיתי אשר נגרם או עלול להיגרם לכם. להלן רשימה חלקית של הפעולות השונות שעליכם לבצע באופן מיידי:
צרו קשר מיידית עם המשטרה ודווחו על האירוע. דאגו לכלול את כול המסמכים אשר עלולים להצביע על כך שזהותך נגנבה. בקשו שהתלונה תעבור לידי היחידה הארצית לחקירות הונאה.
צרו קשר עם בנק ישראל ובאופן פרטני יותר עם כל סניפי הבנקים שבהם אתם מנהלים חשבונות. העבירו להם עותק של התלונה במשטרה עם מסמכים רלוונטיים נוספים לעניין.
העבירו את טופס התלונה במשטרה, ובנוסף פירוט מלא בכתב, לגופים הבאים:
חברות האשראי השונות, גם אלו בהן אין לכם חשבונות, רשות הדואר, משרד הרישוי, משרד הפנים, ומקומות נוספים בהם שמכם מופיע במאגר נתונים כלשהו. חשוב ביותר לתעד ולשמור על כל פניותיכם לרשויות השונות באופן שתוכלו להוכיח באם תתבקשו כי אכן הוגשה תלונה מסודרת וכד'

---

[4] http://www.articles.co.il/article/18977/%D7%92%D7%A0%D7%99%D7%91%D7%AA%20%D7%96%D7%94%D7%95%D7%AA%20-%20%D7%9E%D7%9B%D7%94%20%D7%A2%D7%95%D7%9C%D7%9E%D7%99%D7%AA

<u>מערך שיעור בנושא: גניבת זהויות באינטרנט</u>

נושא השיעור: גניבת זהות באינטרנט

משך השיעור: שעה וחצי (90 דקות)

מיועד לכיתה: השיעור מיועד לתלמידי תיכון בכיתות י"א-י"ב הלומדים בתיכון עירוני א' לאומנויות. השיעור נותן במסגרת פרויקט "אינטרנט בטוח" אשר חושף את התלמידים לסכנות השונות הקיימות בסביבה האינטרנטית.

הרכב אוכלוסייה: הטרוגני.

ידע קודם נדרש ורלוונטי: גלישה בסיסית באינטרנט ושימוש בתוכנת הדואר האלקטרוני השונים.

עזרי הוראה לכלל הכיתה: כיתת מחשבים עם עדיפות למחשב לכל ילד, סרטון תוצאות גניבת זהויות ומכתב phishing לדוגמא.

אסטרטגיות הוראה: פרונטאלית קבוצתית- השיעור ישלב בין הסבר פרונטאלי של המורה תוך הצגת דוגמאות רלוונטיות לנושא לבין לימוד עצמי וחשיפה של התלמיד לסכנות השונות בגניבת זהויות.

מטרות לימודיות:

1. התלמיד יגדיר מהי גניבת זהויות באינטרנט.
2. התלמיד יבחין בסכנות השונות בחשיפת פרטים באינטרנט.
3. התלמיד יתנסה בשימוש נכון של תוכנת הדואר האלקטרוני.
4. התלמיד יבחין בין הודעת דואר אלקטרונית תקינה לבין הודעת דואר קלוקלת.
5. התלמיד יבחין בין פרטים רגישים למסירה לבין פרטים אשר אינם מהווים סכנה.

מטרות חינוכיות:

1. חינוך לצריכה ביקורתית ומושכלת של אינטרנט.

מבנה השיעור	מהלך השיעור	הערות ושיקולי דעת
יצירת מוכנות 10 דקות	התלמידים יתבקשו לפתוח את הדואר האלקטרוני שלהם, כאשר בתוך הדואר יחכה להם הודעה אטרקטיבית ומושכת (כגון מחפשים איך לעבור את הבגרות הזאת?) ובתוכה בקשה לנתינת פרטים אישיים בכדי לקבל את השירות. המורה תסביר בכמה מילים על הדואר האלקטרוני ומרכיביו הבסיסיים (דואר נכנס , דואר יוצא וצירוף קבצים להודעה).	
קישור לנושא 5 דקות	"מי מכם פתח את ההודעה שחיכתה לו במייל ונתן את פרטיו האישיים? כל מי שעשה זאת נפל כרגע כקורבן לגניבת זהות."	יש לשים לב גם לתלמידים שלא פתחו את ההודעה ולשאול אותם מדוע לא פתחו?
גוף השיעור- פעילות מעשית 20 דקות	* צפייה בסרטון בו מספרים אנשים על תוצאות גניבת הזהות שחוו – <u>אילו שימושים נעשו עם גניבת הזהות?</u> כתיבת נקודות השימוש על הלוח כפי שנאמרו מפי התלמידים * המורה מראה את ההבדלים בין המכתב שנשלח לכתובת המציאותית ביחד הם מנסים לעלות על הדברים השונים והדומים	
הערכת ביניים 5 דקות	הגדרת המושג גניבת זהויות מתוך התלמידים ע"י הכוונה בשאלות.	
המשך גוף השיעור 30 דקות	* הסבר כיצד נמנעים מגניבת זהות ונתינת קריטריונים ודוגמאות לבדיקת הודעות דואר אלקטרוניות שונות * מקומות נוספים בהם ניתן לגנוב מידע כגון: צ'אט והגדרת 3 הפרטים החשובים ביותר אותם אסור למסור: ת"ז מספר חשבון בנק ומספר כרטיס אשראי.	

הערכה מסכמת 10 דקות	האינטרנט רווי באנשים ובנוכלים אשר לא מפסיקים להמציא עצמם ומטרתם העיקרית היא להשתמש בשמו ובפרטיו של האחר. בכדי ליהנות מעולמות שונים עלינו לזכור ש: * כשאנו מקבלים הודעה אלקטרונית ממקור לא ידוע כיצד אנו מתנהגים? * כאשר אנו מדברים עם אדם זר איזה פרטים אסור לנו למסור? אם נזכור דברים אלה נמנע מנפילה לתוך רשת גניבת הזהויות הקיימת באינטרנט.	

ביבליוגרפיה:

http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html#Howto

/http://www.idtheftcenter.org

http://www.gov.il/FirstGov/SafeSurfing/General/SSStealingIdentityNet

http://www.microsoft.com/israel/athome/security/email/spear_phishing.mspx

http://www.articles.co.il/article/18977/%D7%92%D7%A0%D7%99%D7%91%D7%AA%20%D7%96%D7%94%D7%95%D7%AA%20-%20%D7%9E%D7%9B%D7%94%20%D7%A2%D7%95%D7%9C%D7%9E%D7%99%D7%AA