নাম: _____ তারিখ: _____ নম্বর: _____

ফিশিং আক্রমণ ও সোশ্যাল ইঞ্জিনিয়ারিং

স্পিয়ার ফিশিং, হোয়েলিং প্রতারণা, SPF/DKIM/DMARC প্রোটোকল, প্রেরক স্পুফিং এবং কর্মীদের নিরাপত্তা প্রশিক্ষণ।

ফিশিং আক্রমণ শিক্ষণ পরিচিতি

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে ফিশিং আক্রমণ ও সোশ্যাল ইঞ্জিনিয়ারিং বিষয়ে গাইড করবে। আপনি স্পিয়ার ফিশিং, হোয়েলিং, ডোমেইন স্পুফিং, SPF/DKIM/DMARC প্রোটোকল, লিংক নিরাপত্তা এবং কর্মী সচেতনতা প্রশিক্ষণ সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/phishing-akromon/

আপনার ফিশিং প্রশমন শেখার রোডম্যাপ

- সাধারণ ফিশিং, ভিশিং ও সাপোর্ট পপ-আপ স্ক্যাম শনাক্ত করুন।
- আউট-অব-ব্যান্ড লেনদেন যাচাই পদ্ধতি বাস্তবায়ন করুন।
- স্পুফ করা ডোমেইন ব্লক করতে SPF, DKIM ও DMARC নিয়ম কনফিগার করুন।

ফিশিং আক্রমণ গাইড নির্দেশনা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। ইমেইল প্রমাণীকরণ বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

ফিশিং আক্রমণ ও সোশ্যাল ইঞ্জিনিয়ারিং (ভূমিকা)

ফিশিং আক্রমণ ব্যবহারকারীর লগইন ক্রেডেনশিয়াল হাতিয়ে নিতে লক্ষ্যভিত্তিক বার্তা, হোয়েলিং প্রতারণা ও ডোমেইন স্পুফিং ব্যবহার করে। কর্পোরেট সিস্টেম সুরক্ষিত করতে গেটওয়েতে SPF, DKIM ও DMARC রুল চালু করার পাশাপাশি আউট-অব-ব্যান্ড অনুমোদন ধাপ রাখা দরকার।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. স্পিয়ার ফিশিং কী?**

- A. নির্দিষ্ট ব্যক্তি বা প্রতিষ্ঠানের জন্য সাজানো একটি লক্ষ্যভিত্তিক ফিশিং ইমেইল
- B. লক্ষ লক্ষ এলোমেলো ঠিকানায় পাঠানো ব্যাপক বাল্ক ইমেইল
- C. ওয়েব সার্ভারকে ট্র্যাফিকে প্লাবিত করা একটি নেটওয়ার্ক আক্রমণ
- D. ব্যবহারকারীর রেকর্ডকে লক্ষ্য করা ডাটাবেস নিষ্কাশন কৌশল

2 **2. স্পুফিং ঠেকাতে কোন প্রোটোকল একটি ডোমেইনকে DNS-এ তার অনুমোদিত প্রেরণকারী IP অ্যাড্রেস তালিকাভুক্ত করতে দেয়?**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

3 **3. হোয়েলিং আক্রমণ কী?**

- A. উচ্চ-পরিচিত কর্পোরেট নির্বাহীদের বিশেষভাবে লক্ষ্য করে চালানো ফিশিং ক্যাম্পেইন
- B. ডেটাবেস ব্যাকআপকে লক্ষ্য করে SQL ইনজেকশন আক্রমণ
- C. স্থানীয় এলাকা নেটওয়ার্কের রাউটার যন্ত্রপাতির ফিজিক্যাল চুরি
- D. স্বয়ংক্রিয় ক্রেডেনশিয়াল স্টাফিং ব্রুট-ফোর্স স্ক্যান

4 **4. DKIM কী করে?**

- A. প্রেরকের সত্যতা যাচাই করতে ইমেইলে ক্রিপ্টোগ্রাফিক স্বাক্ষর যোগ করে
- B. ফায়ারওয়ালে ইনকামিং নেটওয়ার্ক প্যাকেট ট্র্যাফিক ব্লক করে
- C. বিশ্রামকালে ডেটাবেস স্টোরেজ ভলিউম এনক্রিপ্ট করে
- D. সিগনেচারভিত্তিক ম্যালওয়্যারের জন্য ইমেইল সংযুক্তি স্ক্যান করে

5 **5. DMARC-এর ভূমিকা কী?**

- A. SPF/DKIM যাচাই ব্যর্থ হলে গ্রহণকারী ইমেইল সার্ভার কী করবে তা নির্দেশ করা
- B. আগে থেকে গণনা করা রেইনবো টেবিল ব্যবহার করে সিস্টেম পাসওয়ার্ড ডিক্রিপ্ট করা
- C. ডেলিভারির আগে ইমেইল সংযুক্তি কমপ্রেস করা
- D. নেটওয়ার্ক রাউটিং প্রবেশ সুবিধা কনফিগার করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. স্পিয়ার ফিশিং নির্ভর করে লক্ষ লক্ষ এলোমেলো ঠিকানায় পাঠানো সাধারণ বাল্ক ইমেইলের ওপর।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. DMARC পলিসি মেইল সার্ভারকে অননুমোদিত স্পুফ করা বার্তা প্রত্যাখ্যান করার নির্দেশ দিতে পারে।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. SPF যাচাই ইমেলের বডির ক্রিপ্টোগ্রাফিক সিগনেচার যাচাই করে কাজ করে।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. হোয়েলিং আক্রমণ ডেটাবেস ফাইলে অ্যাক্সেস পেতে নিম্নপর্যায়ের কর্পোরেট প্রশাসকদের লক্ষ্য করে।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. পেমেন্ট অনুরোধের আউট-অফ-ব্যান্ড যাচাই আর্থিক ওয়্যার ট্রান্সফার প্রতারণা ঠেকাতে সহায়তা করে।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. ব্যক্তিগতকৃত তথ্য নিয়ে নির্দিষ্ট একজন কর্মীকে লক্ষ্য করা হলো _____ ফিশিং।
2. বার্তা বৈধ দেখাতে ইমেইল হেডার জাল করা হলো প্রেরক _____ ।
3. অনুমোদিত মেইল সার্ভার আইপির ডিএনএস রেকর্ড-তালিকা হলো _____ ।
4. প্রেরক যাচাই দেওয়া ইমেইল-স্বাক্ষর মানদণ্ডটি হলো _____ ।
5. ব্যর্থ SPF/DKIM যাচাই প্রত্যাখ্যানের নীতি স্থাপনে ব্যবহৃত হয় _____ ।
6. সি-লেভেল নির্বাহীদের লক্ষ্য করা ফিশিং অভিযানকে বলা হয় _____ ।

পরিভাষা শব্দভাণ্ডার

ওয়াইফাই | ভাইরাস | স্পিয়ার | স্পুফিং | হোয়েলিং | DKIM | DMARC | SPF

এখানে আপনার উত্তর লিখুন:

1.
2.
3.
4.
5.
6.

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

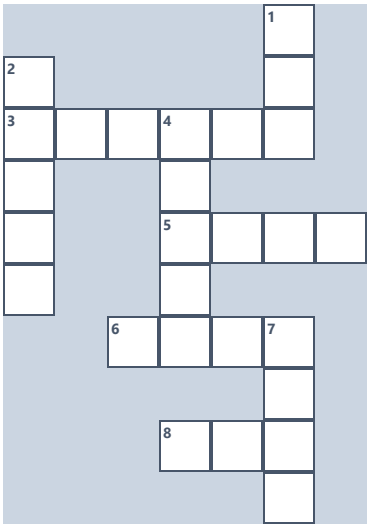
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

____	**1. স্পিয়ার**	**A**	ভয়েসভিত্তিক স্ক্যাম কল।
____	**2. স্পুফিং**	**B**	সি-লেভেল নির্বাহীদের লক্ষ্যবস্তু করা।
____	**3. SPF**	**C**	পলিসি প্রত্যাখ্যান নির্দেশনা।
____	**4. DKIM**	**D**	DNS-এ অনুমোদিত প্রেরক IP।
____	**5. DMARC**	**E**	সোশ্যাল ইঞ্জিনিয়ারিং ইমেইল।
____	**6. হোয়েলিং**	**F**	ব্যক্তিগতকৃত লক্ষ্যভিত্তিক ইমেইল।
____	**7. ফিশিং**	**G**	প্রেরকের ইমেইল ঠিকানা জাল করা।
____	**8. ভিশিং**	**H**	ইমেইলে ক্রিপ্টোগ্রাফিক সিগনেচার।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

3. কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6)

5. ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি (4)

6. নিজেকে নকল করে ছড়িয়ে পড়া ক্ষতিকর কোড (4)

8. প্রত্যাখ্যানের নির্দেশনা-নীতি (3)

উপর-নিচ

1. ব্যক্তিগতকৃত লক্ষ্যভিত্তিক ইমেইল (3)

2. ডিএনএসে অনুমোদিত প্রেরক আইপি (5)

4. তার ছাড়া ইন্টারনেট সংযোগ দেওয়া বেতার প্রযুক্তি (5)

7. ঝুঁকি এড়াতে আগেভাগে নেওয়া মনোযোগ বা ইঙ্গিত (4)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

3 পাশাপাশি: কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6 অক্ষর):

5 পাশাপাশি: ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি (4 অক্ষর):

6 পাশাপাশি: নিজেকে নকল করে ছড়িয়ে পড়া ক্ষতিকর কোড (4 অক্ষর):

8 পাশাপাশি: প্রত্যাখ্যানের নির্দেশনা-নীতি (3 অক্ষর):

উপর-নিচ

1 উপর-নিচ: ব্যক্তিগতকৃত লক্ষ্যভিত্তিক ইমেইল (3 অক্ষর):

2 উপর-নিচ: ডিএনএসে অনুমোদিত প্রেরক আইপি (5 অক্ষর):

4 উপর-নিচ: তার ছাড়া ইন্টারনেট সংযোগ দেওয়া বেতার প্রযুক্তি (5 অক্ষর):

7 উপর-নিচ: ঝুঁকি এড়াতে আগেভাগে নেওয়া মনোযোগ বা ইঙ্গিত (4 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

ই ট লে ছ ণ লে তা বি নি ঘ ল মি কে ভ ড
রা র ঈ তি গ ই সে ভ স মা ণ জে ঘ চ ই
হ ল ণ দ নে স ঝ কা জ ত রা ফ ঘ উ সে
জি ই আ ড প পা ধ দ জি কি র্ক না লি ই রে
ফ মে চ ব দি স শ জা রা দে ট তা মে র ক
সি ই দ ঠ হ ফ সা ও শ মে দে ডি মা র্ক রা
কি ঋ তে না নে ট ছ য য়া প উ অ উ ঋ মা
বা য ফ বা ম ও দে তি ভ ই ঘ রে ষ ফ ঘ
স দ হ স ভ য়্যা রি মি ঢ ষ ফা ষ রি সি না
রা তি তা ড ঊ র নি রা কি থ সে ই ঊ লি গ
ই এ স পি এ ফ নি জা পি ঋ জি লি ট ভ স্পি
ভা ণ জে গ স ঘ রে দি মি ঋ পা উ অ য়া জে
কা গ ম আ ঘ কি ঘ ঝ ণ ধ গ সি র রি শ
ছ দ সে জি নি ঝ রে পে জ আ আ রে মা স মে
তি দে রি ফ সি তি সে খ স বে উ ট সে দি দা

পরিভাষা শব্দতালিকা

স্পিয়ার এসপিএফ ডিমার্ক ইমেইল ভাইরাস ওয়াইফাই সফটওয়্যার সতর্কতা

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. স্পিয়ার

B. এসপিএফ

C. ডিমার্ক

D. ইমেইল

E. ভাইরাস

F. ওয়াইফাই

G. সফটওয়্যার

H. সতর্কতা

সংজ্ঞা ও মিলের ঘর

1. ডিএনএসে অনুমোদিত প্রেরক আইপি।
2. ব্যক্তিগতকৃত লক্ষ্যভিত্তিক ইমেইল।
3. ঝুঁকি এড়াতে আগেভাগে নেওয়া মনোযোগ বা ইঙ্গিত।
4. প্রত্যাখ্যানের নির্দেশনা-নীতি।
5. কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম।
6. নিজেকে নকল করে ছড়িয়ে পড়া ক্ষতিকর কোড।
7. ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি।
8. তার ছাড়া ইন্টারনেট সংযোগ দেওয়া বেতার প্রযুক্তি।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. য়া র স্পি
2. র্ক মা ডি
3. স ভা রা ই
4. র ও ট য়্যা স ফ
5. পি ফ এ এ স
6. ই ল ই মে
7. ফা ই ও ই য়া
8. স তা র্ক ত

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	যেসব ডিভাইস হ্যাক হতে পারে			
2	ফিশিং ইমেইলের লক্ষণ			
3	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
4	ভুয়া জরুরি অবস্থা তৈরি করে এমন শব্দ			
5	প্রেরক যাচাই করার উপায়			
6	IT সাহায্যের জন্য আপনি যাদের জিজ্ঞাসা করতে পারেন			
7	যা যা আপনি ব্যাকআপ করেন			
8	আপনার জানা মাছ বা সামুদ্রিক প্রাণী			
9	প্রতারকরা যেসব কোম্পানির ভান করে			
10	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
11	ভুয়া লিংকে ক্লিক করার পর যা করবেন			
12	ডেটা ফাঁসের পর যা করবেন			
13	যেসব মাধ্যমে ফিশিং ঘটে			
14	যেসব জিনিস আপনি কখনো ইমেইলে পাঠান না			
15	আপনার অ্যাকাউন্ট সুরক্ষিত রাখার উপায়			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: সি-স্যুট হোয়েলিং আক্রমণের প্রতিকার



পরিস্থিতি: একজন Chief Financial Officer CEO-র নাম করে একটি অত্যন্ত ব্যক্তিগতকৃত ইমেইল পান, যাতে একটি গোপনীয় ডোমেইন ক্রয় সম্পন্ন করতে দ্রুত $50,000 ওয়্যার করার অনুরোধ করা হয়েছে।

আলোচনার প্রশ্ন: ব্র্যান্ড স্পুফিংয়ের ঝুঁকি বিশ্লেষণ করুন এবং SPF/DKIM/DMARC ও প্রমাণীকরণ নিয়ন্ত্রণ বিস্তারিত বর্ণনা করুন।

কেস স্টাডি 2: SPF/DKIM/DMARC গেটওয়ে নীতি স্থাপন



পরিস্থিতি: একটি এন্টারপ্রাইজ নিরাপত্তা অডিটে ব্যর্থ হচ্ছে, কারণ আউটবাউন্ড মার্কেটিং ইমেইল প্রায়ই স্প্যাম হিসেবে চিহ্নিত হচ্ছে এবং হ্যাকাররা সক্রিয়ভাবে কোম্পানির ব্র্যান্ড ডোমেইন স্পুফ করছে।

আলোচনার প্রশ্ন: ইমেইলের সত্যতা যাচাই করতে প্রযুক্তিগত ও প্রশাসনিক নিয়ন্ত্রণ প্রতিষ্ঠা করুন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12

খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24

ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36

য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48

ূ=49 ৃ=50 ে=51 ৈ=52 ো=53 ৌ=54 ং=55 ঃ=56 ঁ=57 ্=58 ়=59

14	51	22	10	37	59	51		1	24	46	22	51		42	53	40	58	37	45	39

3	21	58	19	46	31	46	37	59	45	38	46	55		30	38	48	31

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: ফিশিং কী?

ফিশিং একধরনের সোশ্যাল ইঞ্জিনিয়ারিং আক্রমণ, যেখানে অপরাধীরা প্রতারণামূলক বার্তা পাঠিয়ে ব্যবহারকারীদের সংবেদনশীল তথ্য দিতে ভোলায়।

Q2: ফিশিং ও স্পিয়ার ফিশিংয়ের মধ্যে পার্থক্য কী?

ফিশিং সাধারণ বিষয়বস্তু দিয়ে বিস্তৃত গোষ্ঠীকে লক্ষ্য করে, আর স্পিয়ার ফিশিং কাস্টমাইজ করা তথ্য ব্যবহার করে নির্দিষ্ট শিকারকে লক্ষ্য করে।

Q3: হোয়েলিং কী?

হোয়েলিং হলো প্রশাসনিক ক্ষমতাসম্পন্ন উচ্চপদস্থ নির্বাহীদের লক্ষ্য করে চালানো অত্যন্ত লক্ষ্যভিত্তিক ফিশিং আক্রমণ।

Q4: ইমেইল স্পুফিং কী?

ইমেল স্পুফিং হলো জাল প্রেরকের ঠিকানাসহ ইমেল বার্তা তৈরি করা, যাতে প্রাপক উৎসটিকে বিশ্বাস করেন।

Q5: SPF কীভাবে স্পুফিং প্রতিরোধ করে?

এটি DNS-এ অনুমোদিত প্রেরক IP ঠিকানার একটি তালিকা প্রকাশ করে, যাতে গ্রহণকারী সার্ভার মেইলের উৎস যাচাই করতে পারে। [1]

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: DKIM কী?

DomainKeys Identified Mail ইমেল হেডারে ক্রিপ্টোগ্রাফিক স্বাক্ষর যোগ করে, যা প্রমাণ করে একটি ডোমেইন দায়িত্ব নিয়েছে এবং বার্তা বদলানো হয়নি।

Q7: DMARC-এর পূর্ণরূপ কী?

Domain-based Message Authentication, Reporting, and Conformance। [2]

Q8: DMARC পলিসি কী?

SPF/DKIM-এ ব্যর্থ বার্তাগুলোর সঙ্গে মেইল সার্ভার কেমন আচরণ করবে (none, quarantine বা reject), তা জানানো একটি নীতি। [2]

Q9: ভিশিং কী?

ভয়েস ফিশিং, যেখানে আক্রমণকারীরা প্রতারণামূলক ফোন কলের মাধ্যমে প্রশাসনিক বা আর্থিক তথ্য আদায় করে।

Q10: লিংক স্ক্যানার কীভাবে সাহায্য করে?

ক্লিকের সময় গন্তব্য ওয়েব পেজের নিরাপত্তা যাচাই করতে এরা আসা ইমেইলের লিংক স্ক্যান করে এবং নতুন করে লেখে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: হোমোগ্রাফ আক্রমণ কীভাবে কাজ করে?

আক্রমণকারীরা দেখতে অবিকল বৈধ ডোমেইন নামের মতো লাগানোর জন্য একই রকম দেখতে নন-ASCII Unicode অক্ষর দিয়ে ডোমেইন নাম নিবন্ধন করে।

Q2: পিউনিকোড উপস্থাপনা কী?

একটি এনকোডিং, যা Unicode ডোমেইন নামকে 'xn--' দিয়ে শুরু হওয়া ASCII-সামঞ্জস্যপূর্ণ স্ট্রিংয়ে রূপান্তর করে যাতে DNS তা সামলাতে পারে।

Q3: 'p=reject' কেন সবচেয়ে নিরাপদ DMARC অবস্থা?

এটি SMTP সেশনের সময় গ্রহণকারী সার্ভারকে DMARC (সামঞ্জস্যপূর্ণ SPF/DKIM)-এ ব্যর্থ মেইল প্রত্যাখ্যান করতে বলে, ফলে সরাসরি স্পুফিং ব্লক হয়। [2]

Q4: আক্রমণকারীরা কীভাবে SPF রুল এড়িয়ে যায়?

সদৃশ ডোমেইন (টাইপোস্কোয়াটিং) কাজে লাগিয়ে অথবা বৈধ তৃতীয় পক্ষের মেইল সেবায় হ্যাক হওয়া অ্যাকাউন্ট ব্যবহার করে।

Q5: বিজনেস ইমেইল কম্প্রোমাইজ (BEC) কী?

একটি কর্পোরেট প্রতারণা, যেখানে আক্রমণকারীরা ব্যবসায়িক ইমেইল অ্যাকাউন্ট হাইজ্যাক বা ছদ্মবেশে ব্যবহার করে ভুয়া অর্থপ্রদান অনুমোদন করায়।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: মাল্টি-ফ্যাক্টর অথেনটিকেশন কীভাবে ফিশিং ঠেকায়?

এতে দ্বিতীয় স্তরের টোকেন (যেমন হার্ডওয়্যার কী) প্রয়োজন হয়, যা শুধু সদৃশ ল্যান্ডিং পেজের মাধ্যমে চুরি করা যায় না।

Q7: ক্রেডেনশিয়াল হার্ভেস্টিং ল্যান্ডিং পেজ কী?

প্রবেশ করানো ইউজারনেম, পাসওয়ার্ড ও MFA টোকেন রিয়েল টাইমে হাতিয়ে নিতে তৈরি একটি হুবহু একই রকম দেখতে লগইন পোর্টাল।

Q8: সাবডোমেইন হাইজ্যাকিং কী?

একটি অব্যবহৃত DNS সাবডোমেইন পয়েন্টারের নিয়ন্ত্রণ নিয়ে বিশ্বস্ত প্যারেন্ট ডোমেইনের অধীনে ক্ষতিকর ফিশিং ল্যান্ডিং পেজ হোস্ট করা আক্রমণকারী।

Q9: DKIM অ্যালাইনমেন্ট চেক কীভাবে কাজ করে?

এটি যাচাই করে যে 'From' হেডারের ডোমেইন DKIM হেডারে ক্রিপ্টোগ্রাফিকভাবে বার্তায় স্বাক্ষর করা ডোমেইনের সঙ্গে মেলে।

Q10: ইমেইল গেটওয়ের ভূমিকা কী?

ইনকামিং ইমেল ফিল্টার করা, লিংক অডিট করা, সংযুক্তি স্যান্ডবক্স করা এবং SPF/DKIM/DMARC সম্মতি যাচাই করা।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

2025 সালে FBI-র IC3-তে সবচেয়ে বেশি রিপোর্ট হওয়া অপরাধের ধরন ছিল ফিশিং ও স্পুফিং, যেখানে অভিযোগ এসেছিল 191,561টি। [4]

2. নিরাপত্তা ইনসাইট

Business email compromise (BEC) 2025 সালে FBI-এর IC3-তে জানানো $3 বিলিয়নের বেশি ক্ষতির কারণ হয়েছে। [4]

3. নিরাপত্তা ইনসাইট

হোমোগ্রাফ আক্রমণে সিরিলিক হরফের সদৃশ অক্ষর ব্যবহার করে ব্রাউজারে এক্সাক্ট-ম্যাচ ব্র্যান্ড ডোমেইন দৃশ্যত নকল করা হয়।

4. নিরাপত্তা ইনসাইট

'p=reject' থাকলে ডোমেইন প্রাপকদের অনুরোধ করে যাচাইয়ে ব্যর্থ মেইল ডেলিভারির সময় প্রত্যাখ্যান করতে, স্প্যাম হিসেবে জমা না রাখতে। [2]

5. নিরাপত্তা ইনসাইট

CEO-দের লক্ষ্য করা হোয়েলিং আক্রমণ সাধারণত গোপন মার্জার বা ডোমেইন ক্রয়ের জন্য জরুরি পেমেন্ট চায়।

6. নিরাপত্তা ইনসাইট

ক্রেডেনশিয়াল হারভেস্টিং পোর্টাল আসল লগইন পেজের নকল করে, ফলে শিকার সরাসরি আক্রমণকারীর ফর্মে পাসওয়ার্ড লেখে।

7. সিকিউরিটি ইনসাইট

CISA-এর যৌথ ফিশিং নির্দেশিকা DMARC, SPF, DKIM ও ফিশিং-প্রতিরোধী MFA-র পাশাপাশি ব্যবহারকারী প্রশিক্ষণের সুপারিশ করে। [3]

8. সিকিউরিটি ইনসাইট

SPF মূল্যায়ন DNS-কোয়েরি করা 10টি টার্মের মধ্যে সীমিত; সীমা ছাড়ালে 'permerror' ফলাফল আসে। [1]

9. সিকিউরিটি ইনসাইট

FIDO2 হার্ডওয়্যার সিকিউরিটি কী দূরবর্তী ক্রেডেনশিয়াল সংগ্রহের বিরুদ্ধে ক্রিপ্টোগ্রাফিকভাবে সমর্থিত সুরক্ষা দেয়।

10. নিরাপত্তা ইনসাইট

আক্রমণকারীরা প্রথমে কোনো প্রতিষ্ঠানে ঢোকার সবচেয়ে প্রচলিত উপায়গুলোর একটি ফিশিং, তাই নিয়মিত সচেতনতা প্রশিক্ষণ একটি কার্যকর প্রতিরক্ষা।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[1] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 — **সঠিক উত্তর: A**

শিক্ষণ নোট

স্পিয়ার ফিশিং কী? → নির্দিষ্ট ব্যক্তি বা প্রতিষ্ঠানের জন্য সাজানো একটি লক্ষ্যভিত্তিক ফিশিং ইমেইল

2 প্রশ্ন 2 — **সঠিক উত্তর: A**

শিক্ষণ নোট

SPF একটি ডোমেইনের অনুমোদিত প্রেরণকারী হোস্ট DNS-এ প্রকাশ করে, যাতে গ্রাহকেরা এনভেলপ প্রেরক যাচাই করতে পারে।

3 প্রশ্ন 3 — **সঠিক উত্তর: A**

শিক্ষণ নোট

হোয়েলিং আক্রমণ কী? → উচ্চ-পরিচিত কর্পোরেট নির্বাহীদের বিশেষভাবে লক্ষ্য করে চালানো ফিশিং ক্যাম্পেইন

4 প্রশ্ন 4 — **সঠিক উত্তর: A**

শিক্ষণ নোট

DKIM কী করে? → প্রেরকের সত্যতা যাচাই করতে ইমেইলে ক্রিপ্টোগ্রাফিক স্বাক্ষর যোগ করে

5 প্রশ্ন 5 — **সঠিক উত্তর: A**

শিক্ষণ নোট

DMARC-এর ভূমিকা কী? → SPF/DKIM যাচাই ব্যর্থ হলে গ্রহণকারী ইমেইল সার্ভার কী করবে তা নির্দেশ করা

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: সাধারণ গণ-ফিশিংয়ের বিপরীতে স্পিয়ার ফিশিং নির্দিষ্ট ব্যক্তিদের জন্য সাজানো হয়।

7 প্রশ্ন 7 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

DMARC পলিসি মেইল সার্ভারকে অননুমোদিত স্পুফ করা বার্তা প্রত্যাখ্যান করার নির্দেশ দিতে পারে।

8 প্রশ্ন 8 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: SPF প্রেরণকারী IP-কে DNS-এর সঙ্গে মিলিয়ে দেখে; ক্রিপ্টোগ্রাফিক স্বাক্ষর যাচাই করে DKIM।

9 প্রশ্ন 9 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: হোয়েলিং ঊর্ধ্বতন নির্বাহীদের লক্ষ্য করে, যাঁরা পেমেন্ট অনুমোদন ও সংবেদনশীল ডেটায় প্রবেশ করতে পারেন।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: পেমেন্ট অনুরোধ আলাদা, পরিচিত চ্যানেলে নিশ্চিত করা ওয়্যার প্রতারণা ঠেকাতে সহায়তা করে।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

F 1. স্পিয়ার	G 2. স্পুফিং	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. হোয়েলিং	E 7. ফিশিং	A 8. ভিশিং

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 স্পিয়ার	2 স্পুফিং	3 SPF	4 DKIM
5 DMARC	6 হোয়েলিং		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 B – এসপিএফ	2 A – স্পিয়ার	3 H – সতর্কতা	4 C – ডিমার্ক
5 G – সফটওয়্যার	6 E – ভাইরাস	7 D – ইমেইল	8 F – ওয়াইফাই

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা স্পিয়ার, স্পুফিং ও SPF নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

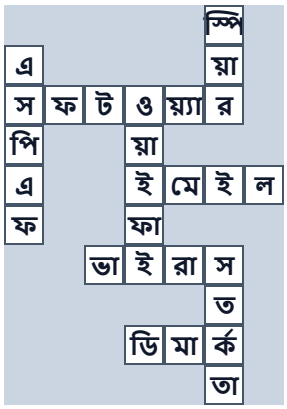
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ই	ট	লে	ছ্	ণ	লে	তা	বি	নি	ঘ	ল	মি	কে	ভ	ড
রা	র	ঈ	তি	গ	ই	সে	ভ	স	মা	ণ	জে	ঘ	চ	ই
হ	ল	ণ	দ	নে	স	ঝ	কা	জ	ত	রা	ফ	ঘ	উ	সে
জি	ই	আ	ড	প	পা	ধ	দ	জি	কি	র্ক	না	লি	ই	রে
ফ	মে	চ	ব	দি	স	শ	জা	রা	দে	ট	তা	মে	র	ক
সি	ই	দ	ঠ	হ	ফ	সা	ও	শ	মে	দে	ডি	মা	র্ক	রা
কি	ঋ	তে	না	নে	ট	ছ্	য	য়া	প	উ	অ	উ	ঋ	মা
বা	য	ফ	বা	ম	ও	দে	তি	ভ	ই	ঘ	রে	ষ	ফ	ঘ
স	দ	হ	স	ভ	য়্যা	রি	মি	ঢ	ষ	ফা	ষ	রি	সি	না
রা	তি	তা	ড	ঊ	র	নি	রা	কি	থ	সে	ই	ঊ	লি	গ
ই	এ	স	পি	এ	ফ	নি	জা	পি	ঋ	জি	লি	ট	ভ	স্পি
ভা	ণ	জে	গ	স	ঘ	রে	দি	মি	ঋ	পা	উ	অ	য়া	জে
কা	গ	ম	আ	ঘ	কি	ঘ	ঝ	ণ	ধ	গ	সি	র	রি	শ
ছ্	দ	সে	জি	নি	ঝ	রে	পে	জ	আ	আ	রে	মা	স	মে
তি	দে	রি	ফ	সি	তি	সে	খ	স	বে	উ	ট	সে	দি	দা

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

3 পাশাপাশি: সফটওয়্যার কম্পিউটারকে কাজ করানোর নির্দেশমালা বা প্রোগ্রাম (6 অক্ষর)

5 পাশাপাশি: ইমেইল ইন্টারনেটের মাধ্যমে পাঠানো বৈদ্যুতিন চিঠি (4 অক্ষর)

6 পাশাপাশি: ভাইরাস নিজেকে নকল করে ছড়িয়ে পড়া ক্ষতিকর কোড (4 অক্ষর)

8 পাশাপাশি: ডিমার্ক প্রত্যাখ্যানের নির্দেশনা-নীতি (3 অক্ষর)

উপর-নিচ

1 উপর-নিচ: স্পিয়ার ব্যক্তিগতকৃত লক্ষ্যভিত্তিক ইমেইল (3 অক্ষর)

2 উপর-নিচ: এসপিএফ ডিএনএসে অনুমোদিত প্রেরক আইপি (5 অক্ষর)

4 উপর-নিচ: ওয়াইফাই তার ছাড়া ইন্টারনেট সংযোগ দেওয়া বেতার প্রযুক্তি (5 অক্ষর)

7 উপর-নিচ: সতর্কতা ঝুঁকি এড়াতে আগেভাগে নেওয়া মনোযোগ বা ইঙ্গিত (4 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1. য়ারস্পি	স্পিয়ার	5. পিফএএস	এসপিএফ
2. র্কমাডি	ডিমার্ক	6. ইলইমে	ইমেইল
3. সভারাই	ভাইরাস	7. ফাইওইয়া	ওয়াইফাই
4. রওটয়্যাসফ	সফটওয়্যার	8. সতার্কত	সতর্কতা

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"গেটওয়ে অডিটে সোশ্যাল ইঞ্জিনিয়ারিং ধরুন"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: সি-স্যুট হোয়েলিং আক্রমণের প্রতিকার

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একজন প্রধান আর্থিক কর্মকর্তা CEO-র নামে একটি অত্যন্ত ব্যক্তিগতকৃত ইমেল পান, যাতে একটি গোপন ডোমেইন ক্রয় সম্পন্ন করতে দ্রুত $50,000 ওয়্যার করার অনুরোধ করা হয়েছে।
- প্রস্তাবিত কৌশল ও সমাধান: স্পুফ করা প্রেরক ডোমেইন ব্লক করতে 'p=reject' পলিসিসহ DMARC কনফিগার করুন। গেটওয়েতে বহিরাগত প্রেরকের সতর্কতা ব্যানার যোগ করুন এবং সব আর্থিক লেনদেনের জন্য মৌখিক, আউট-অব-ব্যান্ড নিশ্চিতকরণ বাধ্যতামূলক করুন।

B কেস স্টাডি 2: SPF/DKIM/DMARC গেটওয়ে নীতি স্থাপন

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি এন্টারপ্রাইজ নিরাপত্তা অডিটে ব্যর্থ হচ্ছে, কারণ তাদের বহির্গামী মার্কেটিং ইমেইল প্রায়ই স্প্যাম হিসেবে চিহ্নিত হচ্ছে এবং হ্যাকাররা সক্রিয়ভাবে কোম্পানির ব্র্যান্ড ডোমেইন স্পুফ করছে।
- প্রস্তাবিত কৌশল ও সমাধান: অনুমোদিত প্রেরকের IP উল্লেখ করে SPF-এর জন্য একটি TXT রেকর্ড প্রকাশ করুন। আউটগোয়িং মেইল সার্ভারে DKIM সাইনিং কী কনফিগার করুন এবং অপব্যবহার শনাক্ত করতে ইনকামিং DMARC XML ফিডব্যাক রিপোর্ট বিশ্লেষণ করুন।